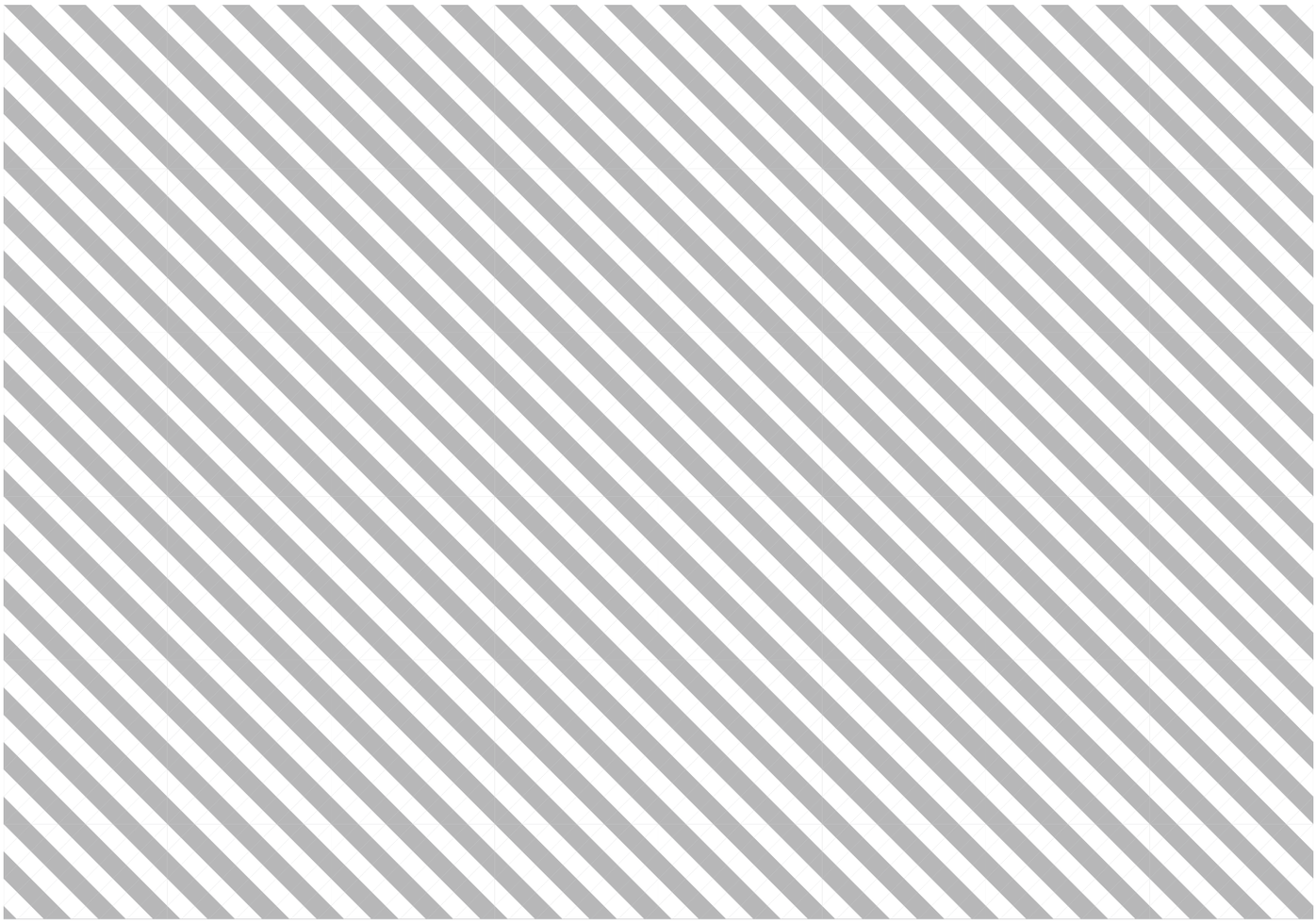
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

APPA – Authorized Public Purpose Access:
Building Trust into Data Flows for Well-being and Innovation

December 2019



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Executive summary

Data: The new oil?

Data is often said to be the oil of the 21st century.[1] Just as new carbon-based fuels powered the original Industrial Revolution, information is driving the Fourth Industrial Revolution. The parallels abound: Data, like oil, must be processed to be useful, and just as oil can explode during refining or leak during transport, data has the potential to cause damage. It is also, like oil, an important factor in geopolitics.

Yet for all their similarities, there are two crucial differences between data and oil. First, data is a nonexclusive commodity – that is, it can be used by multiple actors simultaneously without decreasing in volume or accessibility. And second, when data includes personal information, its collection and use raise questions of privacy and other human rights in ways that the use of oil does not. Data has a positive side, as a tool to create value in the Fourth Industrial Revolution. And it has a dark side: the negative impact on individuals, companies and society that can occur when data is improperly managed and used. The key to managing this negative side and nurturing the beneficial use of data is the establishment of an appropriate data-governance model. In this paper, we discuss the ideal data-governance model in healthcare, a field in which the collection and handling of sensitive personal information plays a central role, and suggest ways in which policy-makers can take the lead in implementing an improved governance model in the real world.

Our challenge

Anecdotes and fables about the search for longevity exist all over the world. The first Qin emperor is said to have sent envoys from China to Mount Fuji in Japan in search of immortality,[2] and the alchemists of medieval Europe sought the life-extending Philosopher's Stone.[3] Today, humans are turning the dream of longevity into reality. Our lifespans, though still finite, are longer than ever before and, in many societies, long lives have become the norm. According to the World Health Organization, by 2030, the average life expectancy in many countries will be over 85 years; in some countries, it will be even longer – the average woman in Korea, for instance, will live past 90.[4] At the same time, problems related to longevity, such as dementia, are emerging as major social issues. According to the WHO, the current number of dementia patients worldwide is 50 million, and this is increasing by one person every three seconds. At the current rate, it will reach 82 million by 2030 and 152 million by 2050.[5] The resulting economic burden on society is projected to increase to $818 billion by 2015 and $2 trillion by 2030.[6]

Japan is a prime example of a "longevity society". The country's life expectancy is among the highest in the world, and the population's average age is rising rapidly. As a result, Japan is on the front line when it comes to dealing with the downsides of longevity, including dementia. In Japan, universal healthcare coverage has been implemented as a social security system for nearly 60 years and, as a result, hospitals and local and national governments possess a large amount of high-quality health-related data.[7] Individuals are also data collectors: Among people in their 60s, the smartphone penetration rate is over 50%,[8] opening up possibilities for the use of real-world data (RWD) collected in various situations by a range of personal devices. In December 2018, the US Food and Drug Administration (FDA) published a framework for its Real-World Evidence Program to support the application of RWD in drug discovery and biotech products.[9] The WHO has also issued guidelines on digital health interventions.[10,11]

This white paper is a product of the Healthcare Data Project at the World Economic Forum Centre for the Fourth Industrial Revolution Japan. The project aims to contribute to the world in two related ways: first, by developing a broadly applicable new model for data governance; second, by applying this model to encourage the sharing and distribution of data (and manage its risks and downsides) in the fight against ageing-related conditions such as dementia, using Japan as a testing ground. Based on our experiences in healthcare, we look forward to extending the discussion to data governance in general.

In order to protect people's human rights when collecting and using their data, it is not sufficient simply to obtain pro forma consent. It is also technically difficult to fully ensure data security by deleting personal information through anonymization. We would like to propose a method for promoting data flows while simultaneously protecting people's rights that is based on values agreed by multiple stakeholders, including individuals.

Findings

The goals of this white paper are as follows:

1. Identify governance gaps in data distribution
2. Describe three crucial factors to be considered when seeking to fill governance gaps
3. Explain Authorized Public Purpose Access (APPA), a proposed concept for data governance focusing on "realizable value"

Findings (overview):

1. Governance gaps in data distribution
   No satisfactory data-governance model has been established to create value through the use of data while appropriately managing its risks. Three of the most important issues that we consider are listed below.

   a. Inadequate personal protection due to an over-focus on consent
   b. Increasingly tight regulations on data-holding companies (companies that use data commercially)
   c. Loss of opportunities to use data

2. Three components of a governance model to drive data distribution
   A governance model that facilitates data distribution should include the following three elements: 1) consideration for individual human rights; 2) consideration for the interests of data holders; and 3) value creation in the public interest. Examples of current data-usage models are provided.

3. APPA: a new proposal for data governance
   As one approach to securing trust and promoting the appropriate use of data, we propose a new governance concept called Authorized Public Purpose Access (APPA), which widens the focus of data-governance mechanisms beyond the explicit, opt-in consent of individuals. We show the advantages of the APPA approach and the expected impact on data use in comparison with current usage and governance models.

Impact

We envision two types of social impact for this project:

1. We hope to facilitate the distribution of data (especially in the healthcare sector), while mitigating the negative impacts of inappropriate data use, by demonstrating the specific components that need to be considered in creating a new governance model.
2. We intend to make Japan a showcase for solving the problems of a "longevity society", which many other countries will face in the future, through the enhanced use of data. Social implementation of solutions will address typical age-related conditions such as dementia, but also go beyond this scope and contribute broadly to the improvement of healthcare services though data.

Governance gaps for data distribution

In the healthcare field, the potential benefits of more and better use of data, especially personal data, are significant. But there are many challenges.[12] Barriers to enhanced data use include: academic competition; the temptation among researchers to hoard data for personal and professional advantage; disparities between the labour required to collect and manage data and the profit to be gained by doing so; the large investments required to fund research activities; the diversity of practices among research areas and researchers; information imbalances among data holders; difficulties in interpreting and understanding shared data; and the scale of resources needed to share and maintain data. Data is both an asset and a liability. Storing it requires physical space for servers and other hardware. Managing it requires human resources. Furthermore, there are legal and economic challenges, such as the time it takes to prepare data for distribution, the money needed to manage the data, and the rights and responsibilities that come with data disclosure and retention.[13]

In general, the market for data-driven businesses is expanding, and some companies that collect and process data, such as the so-called GAFA (Google, Apple, Facebook, Amazon) and BAT (Baidu, Alibaba, Tencent) groups have emerged as powerful economic forces.[14] As privacy awareness grows, there is an increasing need for individual and consumer control over the handling of personal data, including healthcare data, by these companies. It is essential to look out for the interests of individuals, given the impact on their lives, and ensure regulations on such enterprises have been promoted from the perspective of competition laws such as Japan's Antimonopoly Act. But so far, no data-governance model has been established that puts creating value for all stakeholders in society at its core.

We consider three of the most important issues with current models below.

1. Insufficient personal protection due to an over-focus on consent

The first issue is that, when it comes to protecting the human rights of individuals, obtaining consent is not necessarily a panacea. While obtaining consent is important, it poses several challenges.[15] In some cases, it can result in lost value to the person whose consent is sought.

In Japan, the earthquake and tsunami that struck in March 2011 served as a lesson. All Japanese local governments (prefectures, wards and municipalities) have personal information protection ordinances in place. In many cases, such ordinances prohibit the provision of personal information to outside parties, but usually they include exceptions. Although there are differences among local governments, many stipulate that the provision of personal information to outside parties is permitted under

conditions such as: 1) consent of the person in question; 2) specific stipulation by a law or ordinance; 3) urgent and unavoidable need to protect human life, health or property; or 4) after review by a Personal Information Protection Council established by the local government.[16] However, following the 2011 disaster (known in Japan as the Great East Japan Earthquake), when non-government organizations that support people with disabilities requested personal information held by local governments, most governments declined to provide it on the grounds that they did not have consent or that providing the information was unnecessary. Only two local governments, one in Iwate Prefecture and the other in Minamisoma City, Fukushima Prefecture, enabled the provision of outside services based on interpretations of their privacy ordinances by local government departments.[17] Many local governments did not use the provisions of their personal information protection ordinances that allowed for data to be shared, or did not have policies or provisions in place to enable such sharing. Nor could they obtain assessments from Personal Information Protection Councils. (This raises the question: Can and should these councils be convened during a disaster?)

Approximately 60% of the victims of the disaster were aged 65 or older, and the mortality rate of people with disabilities was twice as high as that for healthy people.[18] Thus, it can be said that sufficient support was not provided to vulnerable people.

There is, in addition, the difficulty of making consent-related decisions based on a correct understanding of value. In the first place, consent or agreement on the use of personal data is only one of the potential justifications for using said data. For this reason, the European Union's General Data Protection Regulation (GDPR) requires that legal grounds other than consent be provided,[19] and that consent be obtained in such a way as to make it easier for users to understand the content of data requests and other matters not limited to formal consent.[20] Benoliel and Becher surveyed the readability of 500 of the most popular US website terms and conditions, including Google, Facebook, Uber and Airbnb, and found that 498 of them were of "academic level" difficulty.[21] How many people actually read the terms of service? These documents are long and hard to understand, and if one does not agree, one cannot use the service, putting providers with monopolistic power in a strong position. The use of consent as an indemnification for service providers or a loophole in consumer protection regimes, rather than to further the interests of individuals, can hardly be called good governance. There is also the related problem of "consent fatigue" caused by constant requests for agreement.

Additionally, in the medical field, many patients, such as elderly people, children and some patients under emergency care, have diminished capacity to consent. The Japanese Civil Code, the Act on the Protection of Personal Information and global rules for personal data such as the GDPR do not provide for appropriate decision support for elderly people in cognitive decline, creating the risk that important decisions will be postponed or avoided. Even when consent is possible, we must acknowledge that consent based on it being thoroughly understood is very difficult to achieve. There is an information gap between doctors and patients, and the power relationship between the physician and the patient encourages the granting of consent even when the patient's understanding is imperfect.

2. Increasingly tight regulations on data-holding companies (companies that use data commercially)

The second issue is that, from the perspective of competition law, data-governance models are being introduced that have strong implications for limiting the potential for data use. In the past, the collection of personal information was supposed to be regulated by privacy and consumer protection laws. Competition laws, however, have come to be applied to companies such as GAFA and BAT that use data in the conduct of their businesses (hereinafter referred to as data-holding companies). In 2017, the European Commission fined Google more than €2.4 billion ($2.65 billion) for violating the EU Competition Act in the area of internet advertising.[22] In February 2019, German antitrust authorities determined that Facebook's collection and use of user data, including through its apps, constituted "abuse of a superior position" prohibited by antitrust laws.[23] In Japan as well, in response to this situation, legal regulations on data-holding companies are being considered.[24,25] In addition, there have been moves to impose taxes on the use of data, such as France's Digital Services Tax (DST).[26] Services involving the collection of digital data are increasingly viewed as indispensable in social life. As a result, demands for laws and regulations have emerged in various countries to address the way data-holding companies monopolize data. We are concerned that such developments may lead to an excessive brake on the creation of value through the use of data. We would like to propose a data-governance model in this paper that promotes the use of data even as we debate its risks.

3. Loss of opportunities to use data

The third issue to consider is data-governance models that tend to limit the possibilities of the use of data. At present, the focus of discussion in data governance is on individual privacy and human rights, such as in the GDPR[27] and ePrivacy regulations[28] in Europe, and the National Institute of Standards and Technology (NIST)'s Privacy Protection Framework[29] and the California Consumer Privacy Act (CCPA)[30] in the US. The right to be forgotten has also been demanded out of consideration for individuals. While these rules have been developed with an emphasis on the protection of personal data, the result is often a data-governance model in which data is not used to its full potential. It is important to obtain people's consent when using their data, but sometimes this can result in a failure to realize the data's full value.

In addition to disasters such as the Great East Japan Earthquake, the outbreak of epidemics is another obvious example where such problems could occur. If data is not shared in such cases due to excessive protection of personal information, not only does it harm the public interest, it also harms the interests of the individual data subjects in question.

Additionally, restrictions on cross-border data transfers can have purposes other than privacy protection – such as protecting and promoting the industries of a particular

country; national security; law enforcement and criminal investigations. The GDPR is an example, but increasingly Asian countries such as China and Indonesia are adopting laws and regulations that require data localization and forbid data transfers outside of the country.[31] Such data localization also leads to lost opportunities for value creation through data distribution.

In other words, there is a need for regulations that can facilitate global data sharing. A virtue of the GDPR is that it has created a unified regime for data distribution in the EU in conjunction with countries acknowledged as having sufficiently compatible rules, by consolidating what were once separate rules for each jurisdiction. Additionally, APEC's Cross Border Privacy Rules (CBPR)[32] and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[33] are also frameworks for promoting free data distribution.

In order to address these issues, we propose a framework that: 1) respects the protection of personal information, a fundamental human right as articulated in the GDPR; 2) defines the conditions under which consent can be exempted or consent can be simplified for the purpose of furthering the public interest; and 3) increases the frequency of information distribution and promotes the efficient use of data.

Governance model components to drive data distribution

At the Group of 20 (G20) Summit in held in Osaka, Japan, in June 2019, leaders from around the world discussed how to deal with the rapidly expanding digital economy. They agreed to launch a framework (called the "Osaka Track") to discuss the creation of international rules on the use of data. They agreed, in the Group of 20 Leaders' Declaration, that an idea proposed by Japan called Data Free Flow with Trust (DFFT) could help harness the Digital Economy.[34] DFFT, a framework for data distribution backed by trust, is an important concept that can mitigate the risks of data use.

In the healthcare field, data has been owned by companies, hospitals, municipalities, governments, insurers etc., and access by individuals has been limited. However, in recent years, efforts to secure data-access rights for individual data subjects, such as MyData[35] and Blue Button,[36] have been promoted. Under the GDPR, which took effect in Europe in 2018, individuals now have the right to data portability.

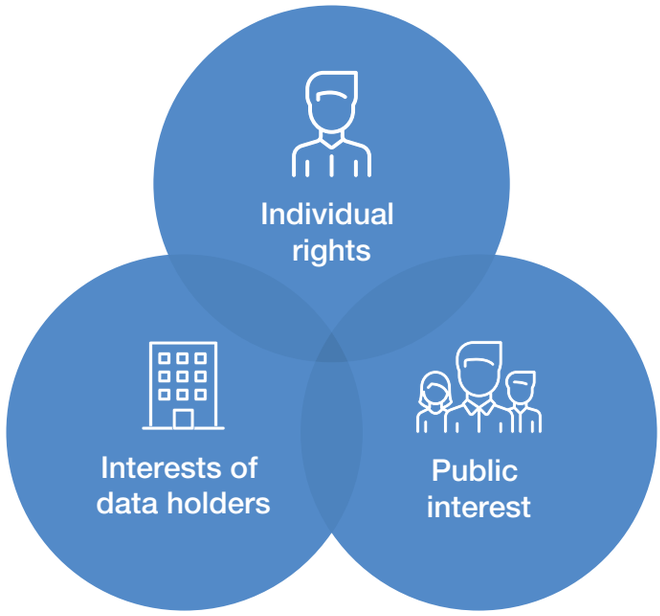
In this way, the axis of data usage is becoming person-centred. Yet at the same time, the limitations of the concept of "data ownership" are becoming apparent.[37] The concept of data ownership has important implications for the right of individuals to influence how their data is used. But it can give rise to misunderstandings such as the assumption that data is something that exists in one place and is subject to exclusive ownership, like oil. This tends to hinder smooth use based on the concept of nonexclusivity. Data is a shareable and copiable commodity that can be combined with other data to increase its value. It is sometimes considered a public good. However, although there are arguments for making data held by academia and the government open (treating it as a public good),[38,39] little progress has been made due to a lack of benefits for holders of data and a lack of clarity regarding the value that could be created though open access to government data.

From what perspective should a data-governance model be built?

Three components of a data-governance model that facilitates data dissemination

To address the three issues arising from governance gaps in data distribution (insufficient individual protection due to an over-focus on consent; increasingly tight regulations on data-holding companies; loss of opportunities to make use of data) and make "data free flow with trust" a reality, we believe the following three elements must be considered (Figure 1).

Figure 1: Data governance key factors



Beauchamp and Childress cite four principles of bioethics: respect for autonomy, non-maleficence, beneficence and justice.[40] However, the present reality of data distribution does not satisfy all four principles. The World Economic Forum, meanwhile, describes six dimensions of trust: security, accountability, transparency, auditability, equity and ethics.[41] We believe that data sharing that satisfies the four principles of bioethics and ensures trust should be promoted.

To that end, the following three factors should be held in balance: 1) consideration for individual rights; 2) the reasonable interests of data holders (those that collect and retain data); 3) realizable value (particularly value that serves the public interest).

The three elements are outlined below.

1. Respect for human rights

The first important element is consideration for the rights of individuals. We will not discuss here what human rights or

individual rights are[42] or why they are important.[43] The GDPR, as a product of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, considers the protection of personal data to be a fundamental human right.[44] Among the four principles of bioethics, the most relevant are respect for autonomy, non-maleficence and beneficence.

Respect for autonomy is a particularly important factor in the use of health data and access to healthcare-related services. The tool used to ensure it is informed consent. There are various ways to make sure people's wishes are respected with respect to the use of their data, including opt-out mechanisms. In recent years, "dynamic consent" has been used by biobanks and so on[45] to ensure that people's intentions are reflected on an ongoing, up-to-date basis.

Consent is an important method for ensuring respect for autonomy, or the right of informational self-determination as it has been established in Germany. However, it should be acknowledged that there are other ways to protect human rights besides consent, which may be insufficient when viewed from the perspective of non-maleficence and beneficence.

Some argue that treating privacy protection as a human right is needed to guarantee trust in the use of data (sometimes described as "privacy as trust"[46]). Some view privacy as derived from a trust relationship.[47] It is also important not only to obtain the consent of the person, but to build privacy protection into systems from the ground up (privacy by design[48]).

When designing a data-governance framework, the following are the main issues to be considered from the perspective of human rights, including the risks and benefits for individuals and other aspects that go beyond privacy. The following list was prepared based on the World Economic Forum's six dimensions of trust, NIST's Privacy Framework Core Structure,[49] the UK's Information Commissioner's Office's Legal Interest Assessment[50] and regulations in Japan.

- Are the benefits for individuals clear? If so, are they appropriately balanced against benefits for the data holder?
- When assessing the potential negative impact on individuals from the processing and use of particular data, do you expect some individuals to be opposed or distrustful?
- Could the data be used in ways that would be impossible for individuals to predict?
- Is consent being obtained appropriately, through an appropriate process?
- Is traceability of data use secured (to ensure transparency)?
- Are there safeguards in place to minimize the (negative) impact that can occur as a result of data handling (anonymous processing, secure computation etc.)?
- Are there any remedies or penalties for information leakage etc.?
- Is the scope of access rights appropriate (with regard to target data or time limits)?
- Have appropriate measures been taken to account for particular characteristics of the data, such as the degree of sensitivity? Does the data include information about people other than the data subject?
- Has the necessity of transactions between individuals and data holders been considered?
  - When the consumer (individual) does not have access to an alternative service
  - When it is practically difficult to stop using the services provided by the relevant data holder even if there are alternative services
  - When the data holder is in a position to influence the price, quality, quantity or any other terms and conditions of the transaction at will to a certain degree

2. Interests of data holders

Second, the reasonable interests of data holders are also important. In realizing value through data processing, it is necessary to consider what makes rational sense for those who hold and manage the data. The four principles of bioethics should be considered, especially in relation to justice. Data cannot be used without the consent of the data holder.

The term "data holder" used here is similar to the concept of a data controller in the GDPR: an entity capable of collecting data, setting access rights to the data and managing the data. In addition to technology companies such as the GAFA group, individuals, countries or international organizations can be data holders. The Open Data initiative is an effort to free data from being owned by data holders and turned into a public good. With such efforts, it is important to build a platform for the proper distribution of data, including standards and protocols for interoperability. In Japan, studies are underway on a mechanism for creating, connecting and opening data called the Person-Centered Open Platform for Wellbeing ("PeOPLe").[51] If one builds an open platform, the big question is how to run it. This element is also important in terms of building sustainable systems.

Article 6 (f) of the GDPR specifies the legitimate interests of data controllers with regard to the use of data. The following are issues for data holders, taking into account the legal interest assessment by the UK Information Commissioner's Office.

- Is there a consensus among data holders?
- Is there a benefit for data holders?
- Can we achieve the same goal without using the data?
- Has consideration been given to the cost required for the data holder to curate the data?
- Has consideration been given to the negative impact on data holders?

3. Public interest

The third element, broadly speaking, is the value that can be realized by using data. This is an important issue when different rights collide – when the right to privacy conflicts with, say, the freedom of expression of others, or the freedom of academic research. Prioritizing researchers' ability to access data might advance the public interest. It should also be noted that the public interest is not limited to the interests of specific countries or companies, but crosses borders – for instance, in measures against infectious disease through the cooperation of multiple countries.

Articles 6 and 9 of the GDPR in Europe and Articles 16, 17 and 23 of the Act on the Protection of Personal Information in Japan stipulate various exceptions regarding the handling of data for public-interest purposes.

To make Data Free Flow with Trust a reality, it is important to consider the broader public interest as well as the interests of individuals (data subjects) and data holders. We believe the legitimacy of legal measures that prioritize the public interest can be ensured though collective agreement and democratic procedures. In Finland[52] and Japan,[53] there have been legislative movements to allow the secondary use of data for medical research, although such movements have been restricted to anonymized data used for limited purposes and handled in a rigidly specified manner.

As with human rights, there are various arguments as to what kind of data rules are appropriate for the public interest. This question is discussed below in more detail, with an explanation of APPA, our proposed governance model. The point we would like to make here is that considerations of the public interest should be prioritized when pursuing important collective projects such as the United Nations' Sustainable Development Goals (SDGs)[54] or universal health coverage.[55] This element also relates to the notions of beneficence and justice in the four principles of bioethics. Issues to be considered from the point of view of the public interest components are listed below.

- What is the public benefit that can be realized? Is it really in the general public interest? Is it linked to freedom of expression and academic research?
- Is the potential positive impact large?
- Is there an appropriate balance between the size of the public benefit to be realized and any negative impact on individuals and/or data holders?
- Is there appropriate agreement among target groups? Has such agreement been sought through an appropriate process?
- Are laws or guidelines in place?
- Is the expectation of public benefit based on sufficient evidence?

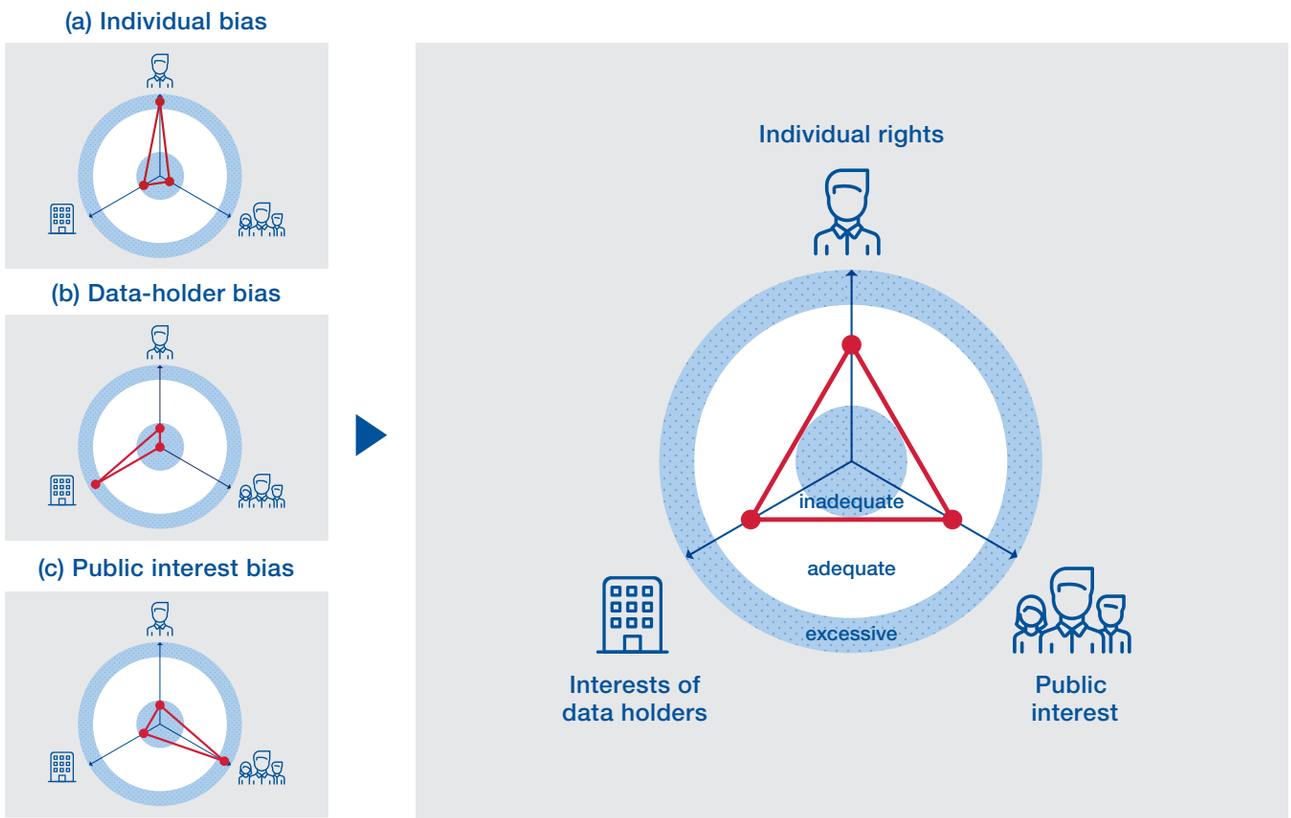
We believe that a data-governance model designed with these three perspectives in mind could promote more efficient sharing and use of data. This does not mean, however, that data should never be used unless all three elements are completely satisfied.

Examples of typical data-use problems based on the three factors

Today, data tends to be used in ways that favour one of the three components. Ideally, all three elements should be satisfied, but in practice, over-prioritizing of one or another of them leads to pitfalls, such as insufficient consideration for human rights or the inability to fully realize data's potential value.

The figures below (Figure 2) illustrate typical bias patterns. Taking appropriate steps to address these imbalances can result in increased trust in the distribution of data.

Figure 2: Typical problem cases



1. Individual bias
The first illustration in Figure 2, case (a), represents an example of inappropriate bias towards individuals.

Consideration for individuals is important, but it can also hamper innovation; the individual might even end up being harmed rather than helped as a result. In extreme cases, such as with behaviours that fall under the so-called "right to be wrong" or "right to be foolish", the freedom of the individual can lead to harm to others[56] (e.g. passive smoking, discussed below).

There is debate over the extent to which individual rights (including the right to be foolish) should be respected in cases where there is a conflict between consideration for the individual and the public interest. But many people agree that a degree of "paternalistic" intervention is justified in certain cases.[57] In Japan, as a result of lessons learned from the Great East Japan Earthquake, the Disaster Countermeasures Basic Act was revised to support those who need assistance in the event of a natural disaster. The revision obliges local governments to create a list of people who need special support, and makes clear that this personal information will be shared during a disaster without any requirement to obtain consent.[58] (In situations where consent can easily be obtained, such exemptions should not be necessary – though, as mentioned above, it is not always clear that consent reflects the actual intention of the person providing it.)

Other examples of tension between individual rights and the public interest include the question of privacy for suspected victims of child abuse and their families (i.e. under what circumstances should it be permissible to share potentially relevant private information with hospitals, administrative authorities or the police) and the treatment of people with dementia. What happens when a person with dementia does not (or cannot) consent to care interventions that are in the public interest (as well as their own)?

It should also be considered that implementing the individual right of information control, the right of data portability and the right to be forgotten entails a large cost for data holders.

2. Data-holder bias
Data holders such as the GAFA technology companies are not charities; they collect and use personal data in the pursuit of profit. When a data business achieves a dominant market position, there is a risk that its activities will come into conflict with competition laws, or that it will otherwise abuse its position for its own interests. The illustration at the bottom left of Figure 2 shows such a case.

As mentioned earlier, Europe has responded by making individuals more involved in managing their own data (under the GDPR), and by strengthening antitrust enforcement. Companies also risk damage to their brands due to public criticism, even when their actions are deemed legal.

In the field of healthcare, a typical case in which individual rights and the public interest are impaired by excessive deference to the interests of data holders involves clinical research. Often, companies keep research results to themselves rather than sharing them with research partners or society. Another case is the use of algorithms to profile people for various purposes, which increases the risk of discrimination and disadvantageous treatment in employment, insurance and other aspects of daily life (a risk addressed by the GDPR's regulations on profiling).[59]

3. Public-interest bias
Typically, national or regional regulations on the handling of personal information, such as the GDPR in Europe and Japan's Personal Information Protection Law, contain exceptions to normal data-processing rules for uses that are in the "public interest" or that promote "public health".[60, 61] Needless to say, extreme prioritization of the interests of society as a whole over those of individuals can also be problematic. "Public interest" is not a magic phrase that justifies any and all use of personal data. It can be used as a pretext for authoritarianism or the creation of a surveillance society. There are genuine, difficult trade-offs to be negotiated between, for example, public safety and individual rights. Critics of state responses to terrorism have argued that some countries have erred too much on the side of the former. Furthermore, it is crucial to distinguish between genuine public interests (those of society as a whole) and those of state institutions or officials, and to seek to create value broadly though international cooperation rather than to pursue narrow national interests.

Appropriate consideration should be given to individuals, data holders and society at large. But there is no panacea. Therefore, as one way to deal with imbalanced problem cases such as those described above, we propose an approach called Authorized Public Purpose Access (APPA), which places special emphasis on value co-creation.

Authorized Public Purpose Access (APPA)

We propose an approach to data governance that promotes the use of data by focusing on "realizable value" for the three constituencies described above (individuals, data holders and society). The concept, which we call Authorized Public Purpose Access (APPA), does not rely solely on the opt-in consent of individuals to protect their human rights.

APPA is defined as follows:

> APPA is a model for realizing value by permitting access to data for specific, agreed public purposes, such as the development of medical care and the improvement of public health, though processes that do not rely exclusively on explicit, individual consent as a means of protecting human rights.

It is difficult to protect the rights of individual data subjects while simultaneously avoiding opportunity costs arising from reduced data sharing and usage, and excessive burdens on data holders. Measures that cause anxiety and distrust among individuals and data holders cannot be called appropriate even if they are legally sound. Some governance models emphasize individual control by focusing on the securing of appropriate consent, while others seek to minimize privacy risks and ensure security by mandating anonymous processing and encryption. Our approach emphasizes the value that can be created, assuming appropriate procedural guarantees.

In the field of healthcare, the principle of beneficence (mentioned above as one of the four principles of bioethics) implies a particularly strong obligation to further the public interest. This does not, of course, mean that restrictions on access to data should be lifted entirely in the name of serving that interest.

Access to data under an APPA model should be limited to specific purposes that have been defined through a process of broad public agreement, critique and verification, respecting the human rights of minorities and not favouring the interests of particular groups or states. In addition, it should be noted that APPA can also cover efforts to promote open data and distribution (which mostly assume data anonymization).

APPA does not mean that all data should be treated as a public good or managed by public authorities. Like the concept of "privacy by design", it is based on the idea that public data access should be allowed in a way that guarantees trust and individual human rights (based on appropriate agreement).

APPA implies that prevailing models of data distribution and use, which are too easily bound to the concept of exclusive ownership, should shift their emphasis to data nonexclusivity and access rights. For example, one legal mechanism that is compatible with APPA is the "award-granting nonexclusive licence" provision in the Japanese Patent Act.[62] The provision allows third parties to use patented information for important public purposes, or if the patent holder has failed to make actual use of the patent.

It is also important to prevent the unintended spread of data by focusing on access-right control based on the use of common IDs and blockchain technology in distributed databases.

Specific APPA-compliant provisions will depend on the use case, but should take into account the three components listed above. That is to say: Are human rights and personal autonomy protected (through methods including but not necessarily limited to consent)? Are demands on data holders reasonable? And is there a legitimate, well-grounded public-interest purpose involved?

For more specific applications of APPA, the direction being set by the research community with regards to data sharing, described below, will be helpful. Though this proposal does not focus only on the smooth use of data, it goes without saying that it should not be applied in ways that create new obstacles to data use.

Normally, if the requirements of the party that wishes to use a particular set of data match the basic conditions for such use set by the data holder, access rights will be granted automatically. In cases where the public interest is clear and urgent, such as saving lives in the event of a disaster, data access should be allowed without special prior review. In addition, data access based on democratically adopted laws should be allowed, assuming transparency and accountability are ensured. Alternatively, we believe that data access should be allowed if appropriate prior screening procedures and follow-up reviews are performed, and it can be objectively demonstrated that consideration for the three governance elements described in this paper has been built into the system's architecture.

Use of data without consent? Discussions related to the concept of APPA

APPA is an attempt to emphasize collective agreement rather than individual consent. The GDPR also shows that consent is not the only way to guarantee individual human rights. In research ethics, informed consent is ranked sixth of the seven ethical requirements[63] proposed by Emanuel et al. of the National Institutes of Health in the United States. A research project is not automatically ethical simply because the researcher has obtained consent from his or her subject. According to Emanuel, the first and most important consideration should be social or scientific value – the value that can be realized by the research. It is considered ethically problematic if, even with individual consent, the study lacks value, an appropriate balance of risks and benefits or scientific validity. Emmanuel's governance model, like APPA, does not necessarily rely on individual consent.

Suppression of individual freedom (including the right to be foolish) is already practised in the real world under the law, in cases where individual actions negatively affect the public interest (especially the human rights of others). Take smoking, for example. There is solid evidence that passive smoking increases the risk of lung cancer. Measures to prevent passive smoking are being taken worldwide, for example, through the WHO's Framework Convention on Tobacco Control (FCTC).[64] In order to reduce passive smoking in workplaces and restaurants, an increasing number of companies have eliminated smoking areas or prohibited smoking at certain times of day. This idea can be applied to data use; The use of data to prevent negative impacts on the public interest should not necessarily be premised on individual consent. Law professor Lawrence Lessig points out that trying to perfect individual consent mechanisms in an architecture that needs to be built for reliable data distribution is a misguided strategy.[65] "Users don't really understand how the data is used; they're used to constantly telling small lies about reading and agreeing to the terms when they don't really mean it, and they know that giving people the power to exercise their free will doesn't actually represent anyone's will," he warns.

In other words, the area to be judged by the user should be made as small as possible. He also points out that individual decisions are not necessarily the choices you want to make collectively; individuals are weak people who want to eat sweets when they are hungry even though they know they are unhealthy. It is hard to believe that society as a whole will move in the right direction if it is left to them to decide how to use data. Therefore, policies are needed to regulate the use of data. In Japan, for instance, the law was amended in 2019 to make it possible for researchers in the fields of medicine and long-term care to use public databases for public-interest purposes.[66]

Sunstein's concept of "choosing not to choose"[67] may also be important, given that it can be impossible in practice for individuals to choose, especially in healthcare where information asymmetry makes it difficult for patients to make decisions. Often, the only answer is to leave the choice to someone you can trust.

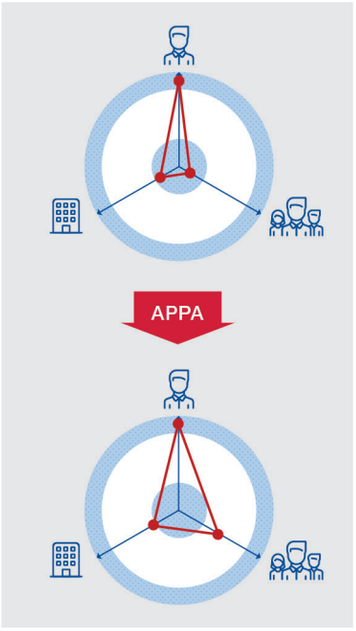
The basic idea behind APPA is that governance mechanisms need not necessarily be based only on the consent of individuals, but may also take into account the value that can be realized – by authorities such as national or local governments, for instance, or by companies – by using the data. This is in part related to the long debate over constraints on human rights imposed by governments in the name of the public interest. Regarding the legitimacy of state authority, the legal philosopher Joseph Raz offers the "normal justification thesis", which states that legitimate authority derives from a situation where subjects are likely to be better off by following the authority's directives than by weighing, assessing and deciding for themselves.[68] Raz's concept of "exclusionary reasons" requires that parties to a dispute comply with the decision of an arbitrator instead of following their own reasons for action (first-order reasons).[69] Alternatively, Andrei Marmor, another legal philosopher, has argued that obeying the orders of the state can lead to better outcomes than thinking and acting on one's own.[70]

In other words, states possess legitimate authority precisely because of their ability to promote public welfare through technical expertise. This point can be said to be connected to the concept of APPA.

There has been some debate about the relationship between collective agreement and democracy, including Rawls,[71, 72] but we will not delve into that here.

Finally, some have tried to solve the dilemma of consent by mandating anonymization. However, anonymized data always carries the risk of re-identification.[73] It seems possible to minimize the risk to privacy though encryption, secure computation and other technical methods, but these tools are not all-powerful. Consideration of the three governance elements is crucial.

1. Applying APPA to correct for individual bias and realize new value



The APPA approach makes it possible to achieve public-interest benefits that have not been fully realized due to an excessive focus on individuals, especially the prioritization of consent. APPA-based governance must still pay attention to individual human rights (in terms not limited to consent) and the minimum interests of data holders. APPA-based mechanisms presume that normal consent-securing methods are not viable – APPA does not need to be applied where true consent of the data subject or data holder is obtainable.

An APPA to data governance would be particularly beneficial in situations such as the three cases outlined below.

a. First, where there is a clear potential benefit for the individual but direct consent cannot be obtained, and implied consent can be presumed based on a rational evaluation of the situation.

   Normally, having one's behaviour restricted is unpleasant and stressful (even if there is clear evidence that many people will not want to constrain the behaviour harmful to their health, such as smoking or consuming too

much salt). Yet many public health rules seek to do just that. Singapore, for instance, has announced a policy banning all advertising of packaged sugary drinks.[74] It is important, however, that they do not ban the sale of sweetened beverages to people with diabetes. Individual freedom, including the right to be foolish, must be recognized as valid, even if it is balanced by other considerations. APPA-based data access should be allowed only in limited cases, and to an appropriate extent, where the benefits accrue to both the individual and society, such as in cases where dementia or other conditions have impaired a person's cognition or decision-making capacity, or in an emergency situation such as a natural disaster where there is insufficient time to confirm individual intent.

b. Second, when respecting the will of the individual increases the risk of harm to others.

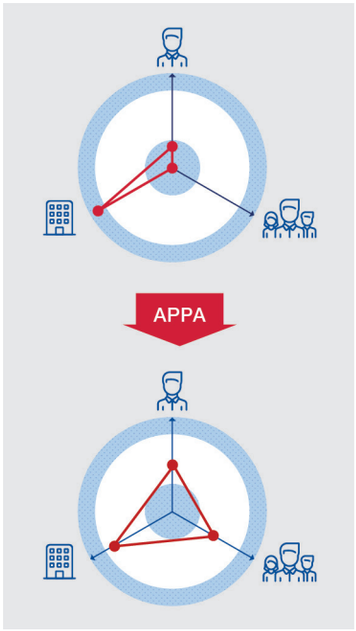
   The FCTC's approach to passive-smoking prevention is presented as a risk-oriented approach. Similarly, data may also need to be used to protect others. For example, in order to prevent child abuse, people who believe there is risk that a child is being abused should be allowed to share personal information (information on the parents of the child) with local governments.[75] Obviously, parents who abuse their children cannot be expected to consent to such data sharing. It should be noted that these risk-based, paternalistic interventions may lead to constraints on individuals (for a legitimate reason). APPA applications should be limited to cases where there is sufficient evidence for the risk being addressed, and where addressing it would lead to the realization of significant value (related to, for instance, SDGs or universal health coverage).

c. Third, consent decisions can be difficult to make for non-experts (or even experts). Over-emphasizing consent can, paradoxically, lead to careless decisions. Careful judgements need be made about risk to the individual based on broadly agreed criteria. In this case, as Sunstein says, some kind of paternalistic use of data in order to protect the individual might be valid if the individual "chooses not to choose".

   A related argument involves elderly people with dementia. People with dementia may have difficulty managing their property, or they may have a propensity to wander off. In such cases, family members might consider using GPS devices or other tools to keep track of possessions and guard against wandering.[76] For people with dementia, this can lead to an unpleasant feeling of being monitored. On the other hand, care fatigue among family members has become a social issue, with consequences such as loss of work, suicide and questions of responsibility for accidents involving the dementia sufferers they care for.[77] The purpose of APPA is to balance risks and benefits. But that involves difficult judgements and, in many cases, it is appropriate not only to obtain the consent of the individual in question, but also of all concerned parties. Regardless, the scope of access to data should be appropriately limited when sensitive information such as a dementia diagnosis is involved.

   In any of these cases, there is a risk that performance and/or sustainability might be compromised due to excessive burdens on data holders. Some form of incentive design for data holders is required. If the data holder is a national or public entity, implementation may be a public service; in this case, the bias might be towards the public interest rather than towards the data holder per se.

2. Applying APPA to correct for data-holder bias and realize new value



The APPA approach can be effective in promoting the beneficial use of data held by companies, nations or academia. It should be noted that this does not mean promoting data use by holders who simply proclaim that they are acting in the public interest (when in fact the use might impinge on human rights).

The following two APPA use cases might be typical.

a. When public-private partnership is important for the realization of public-interest goals such as SDGs

   We believe there are areas where the APPA model should be applied to data use in public/private partnerships (PPPs).[78] PPPs are a method for solving social problems through partnerships between the public and private sectors. They have their origin in the privatization of national services (water, electricity, gas, telecommunications, railways etc.) under the Conservative government of Margaret Thatcher in Britain, which was inaugurated in 1979 with the aim of "greater public benefit though smaller government".[79] Recently, however, more nuanced tools such as Social Impact Bonds (SIBs) have attracted attention. It is now widely accepted that the expertise and financial resources of the private sector can be used to contribute to the public interest. In PPP efforts, including SIBs, the purpose is to serve the public interest in areas such as the provision of public goods; the role of the private sector is to carry out the project in a sustainable way. Applying the concept

of APPA to PPPs established by central and local governments, following the appropriate processes, could help ensure such initiatives' public-interest value.

Private companies are sometimes criticized for extracting too much profit from PPPs.[80] To forestall such criticism, social consensus is critical, and placing certain limits on the interests of data holders may be appropriate. For example, it is possible to avoid excessive profit-taking by restricting profit margins to an appropriate level, or to use PPPs in areas that are not inherently highly profitable. In some cases, data holders may be allowed to use data without individual consent if the necessary public consensus existed and doing so were needed to serve the public interest or the reasonable interests of the data holder. In areas related to the achievement of the SDGs, for instance, such an approach could promote better use of data in low-profit businesses where the rational judgement of data holders alone would not be sufficient (for example, in the fight against rare diseases), or where there is the potential for valuable new uses of data that have not previously been possible with the requirement of individual consent. This is also an important perspective in implementing the value in a healthcare framework for value-based health systems.[81]

b. When pursuing new value that can be shared broadly by humanity, such as medical research

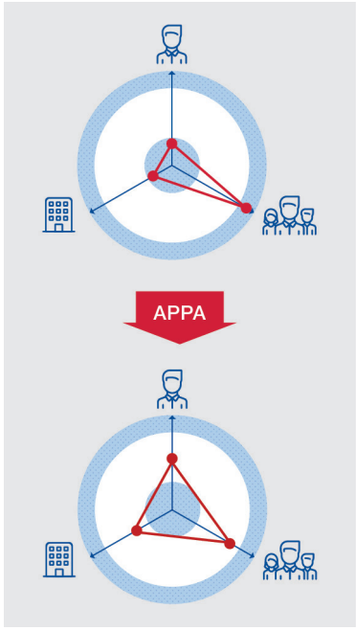
Various efforts are being made for data sharing at the research level, including open data distribution. The Undiagnosed Diseases Program,[82] proposed by William Gahl of the National Institutes of Health (NIH) in the United States, promotes the sharing of data on undiagnosed diseases. In Japan, the Initiative on Rare and Undiagnosed Diseases (IRUD),[83] led by the Japan Agency for Medical Research and Development (AMED), has begun a similar initiative. In order to identify undiagnosed diseases, it is necessary to find similar cases, but there is a limit to the ability of doctors to do so on their own. The Matchmaker Exchange (MME),[84] an international case-comparison platform for undiagnosed diseases, is leading global efforts to confirm the identification of undiagnosed diseases through data sharing by linking undiagnosed-case databases in North America, Europe and the Asia-Pacific region. However, benefits for data holders, such as hospitals and doctors with patient data, have not been fully provided in this initiative. It has been left to highly motivated doctors and professors to gradually expand the effort, driven by the potential for significant public benefit. One challenge for data sharing related to undiagnosed disease is how to design a system that ensures benefits for data holders.

When it comes to genomic information, the Global Alliance for Genomics and Health (GA4GH) has proposed a new governance model called the "registered access policy model" for sharing data obtained though research among research groups or third parties.[85] GA4GH is an international cooperative organization whose goal is to construct a basic framework to enable the sharing of genomic information with the consent of research participants and the protection of personal information. Its efforts could serve as another model for APPA-based data governance.

In the area of legal reform, the World Economic Forum Centre for the Fourth Industrial Revolution Japan is aiming to incorporate the concept of APPA into legal revisions in Japan, and is working on a governance model to enable the secondary use of data obtained through AMED-initiated research programmes. Data is important in healthcare to demonstrate both the development and the implementation of social systems that provide value to society. Our goal is to build a data-governance model and implement it in the public arena to promote open innovation among industry, academia and governments, taking into consideration the interests of individuals, data holders and the public.

Increasingly, as seen in debates about the Human Genome Project,[86] there is a need to consider the balance between what should be common human assets, corporate interests and individual human rights, and to control access appropriately.

3. Applying APPA to correct for public-interest bias and realize new value



The APPA approach does not endorse removing all limits to data use in the name of serving the public interest. A particularly critical point is that narrow national interests, or the interest of state institutions or officials, should not be conflated with the true public interest. One defining feature of APPA-based governance is that applications must be developed and implemented through consensus-building. We believe that broadly based agreement can sometimes pre-empt the need for explicit consent in ensuring the protection of human rights and the legitimate interests of data holders.

Even under current laws and regulations, the use of personal data without consent is sometimes permitted under certain conditions. But excessive restrictions on human rights imposed for reasons such as national security can create unreasonable barriers to data use.

Below are two examples where APPA could apply.

a. Cases involving national or local governments

States sometimes monitor individuals for purposes of national security. Edward Snowden's revelations about the NSA's International Surveillance Network (PRISM) caused a sensation and influenced the creation of the GDPR.[87] Surveillance that fails to gain trust can lead to human rights violations, and not just by intelligence agencies. Information sharing among professionals is important in medical care, and there are many situations in which access to information held by government institutions is required, such as to prevent domestic abuse or take countermeasures against illegal drugs or infectious diseases. Also, measures to prevent terrorism against medical institutions are easily justified, given the risk to human life. However, it is important to guard against policies that go beyond the needs of health or security and violate human rights, or opaque and unaccountable uses of data that lead to discrimination. For example, in Estonia, access to healthcare data at the national level is facilitated by blockchain technology, but unnecessary government access is prohibited, and individual data subjects can find out who has accessed their information, which information has been accessed and for what purpose.[88] APPA-based models should promote transparency and accountability, strictly prohibit unnecessary data access, and promote trust.

b. Cases involving international organizations

When data is shared via the internet, entities with international platforms often become data holders. Since data distribution is not confined to a single country, there may be cases in which international organizations such as the WHO control the use of data across borders. The GDPR, APEC's Cross Border Privacy Rules (CBPR) and DFFT seek to set rules for cross-country data distribution. The United Nations Relief and Works Agency for Palestine Refugees (UNRWA), for example, is currently developing an eHealth system for Palestinian refugees,[89] which is a good example of serving the public interest across countries. Another case of an APPA-style model would be an international information collaboration to combat infectious diseases. When linking information, it is important to ensure interoperability to avoid unnecessary monopolization of data. Standardization of data-related terminology is also important.[90]

Considerations in the APPA model

The idea that consent can sometimes be disregarded does not mean that individual human rights can be sacrificed in the name of national interests or public morality. Inappropriate use of data negatively affects not only individuals but also society as a whole. There is much debate about the nature of justice and the relationship between freedom and order,[91, 92, 93] but the value realized though APPA needs to be compatible with freedom, and to serve the true public interest, not a pretence of it. Even when public-interest motives are sincere, applications should be confirmed and corrected through constant verification, and should not simply be accepted as products of altruism or good morals.[94]

We also believe that appropriate processes need to be followed that take into account the nature of the data to be used and the likely impact on individuals. Potential processes for creating APPA-based systems include referendums, legislation, ordinances, third-party opinions, guidelines and so on. The appropriate process will vary depending on the extent of the effect on the individual and the public interest.

When multiparty agreements or third-party assessments are used in place of consent, and the circumstances or views of the data subject change over time, issues can arise involving the continued reasonableness of the initial agreement or the legitimacy of the third-party judgement. We believe that the reliability of APPA models will be enhanced through feedback from real-world models and further discussion of the appropriate handling of the three elements discussed in this paper.

In addition, although APPA is defined here with the use of data in the healthcare field in mind, we believe that it is a concept that can be extended to the use of data in other fields in which the public interest plays a significant role.

Conclusion

Major benefits are expected from enhanced use of data in healthcare. This paper presents concrete components for an appropriate data-governance model and proposes APPA as a model for appropriate data governance.

Through APPA, we hope to:

– Facilitate data distribution (especially in the healthcare sector) while mitigating the negative effects of inappropriate data use by indicating the specific components needed for an appropriate governance model.
– Promote social implementation of data-use models, beginning in Japan, that contribute to the development of a wider range of healthcare services and address problems related to “longevity societies”, such as dementia and other ageing-related diseases.

In addition to promoting the well-being of elderly people in a longevity society, there is also the possibility of using APPA for a wide range of data-driven initiatives, including achieving the SDGs.[95]

The following points need further discussion in the future:

– Building economically sustainable models. There is a high possibility that the beneficiaries of services based on enhanced use of data, such as those with dementia, elderly patients and low-income individuals may not be able to bear the costs
– Developing specific methods by which appropriate consent can be obtained (not limited to APPA). Consent can be managed by consent management platforms for efficiency, but there is also the possibility of using artificial intelligence (AI) to support decision-making (personal AI agents, etc.)
– Using AI in the medical field, including intellectual property and professional responsibility
– Minimizing privacy risk. Creating value with data while respecting privacy by, for instance, applying access control and secure computation technologies, use of data for machine-learning AI algorithms only etc.
– Cybersecurity for APPA
– Creating an environment where service providers can share data. It may be possible for companies to create a “smart city”-type community on a virtual basis. Shared rules for interoperability would be needed
– Building a new architecture based on Globalization 4.0.[96] For instance, the introduction of federated data systems[97]

These issues will be discussed in future reports. In the meantime, we look forward to feedback, opinions and continued discussion among a wide range of stakeholders.

Contributors

Healthcare Data Policy, Centre for the Fourth Industrial Revolution Japan, World Economic Forum

Takanori Fujita, Project Lead
Seiichiro Yamamoto, Project Lead
Jonathan Soble, Editorial and Communication Lead
Hiroaki Atsuji, Fellow, Takeda Pharmaceutical
Yosuke Horii, Fellow, Eisai
Keisuke Naito, Fellow, Eisai
Masako Okamoto, Fellow, Mitsubishi Tanabe Pharma
Reiko Onodera, Fellow, Takeda Pharmaceutical
Yasunori Suzue, Fellow, Sompo Holdings

Hiroaki Miyata, Professor, Keio University School of Medicine
Yuko Tanaka, Senior Manager, 1st Government and Public Solutions Division, NEC

Acknowledgements

We would like to thank the academics, professionals and everyone who contributed significant time in meetings and reviews to produce and refine the content, frameworks and conclusions of this white paper.

Nagisa Asano, Student, The University of Tokyo Faculty of Law
Yoichiro Itakura, Partner Lawyer, Hikari Sogoh Law Offices
Fumiko Kudo, Visiting Researcher, The University of Tokyo Institute for Future Initiatives
Tasuku Mizuno, Partner Lawyer, City Lights Law
Shinsuke Muto, Co-founder, Tetsuyu Healthcare Holdings
Takafumi Ochiai, Partner Lawyer, Atsumi & Sakai
Takehiro Ohya, Professor, Keio University Faculty of Law
Kohei Onozaki, Board Member, Health and Global Policy Institute
Seiya Sasaki, Student, Keio University Graduate School of Law
Kenji Shibuya, Professor and Director, Institute for Population Health, King's College London
Akihisa Shiozaki, Partner Lawyer, Nagashima Ohno & Tsunematsu
Akira Takubo, Graphic Designer, Takubo Design Studio
Masako Toriya, Project Senior Assistant Professor, Keio University Graduate School of System Design and Management
Takayuki Ueki, Project Researcher, The University of Tokyo Institute for Future Initiatives
Tatsuhiko Yamamoto, Professor, Keio University Law School
Makoto Yamasaki, Project Assistant Professor, Keio University Graduate School of System Design and Management
Shigeto Yonemura, Professor, The University of Tokyo Faculty of Law and Graduate Schools for Law and Politics

Eisai
Mitsubishi Chemical Holdings
NEC
Sompo Care
Sompo Holdings
Takeda Pharmaceutical

Endnotes

1. “The world’s most valuable resource is no longer oil, but data”, The Economist, 6 May 2017: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (link as of 2/12/19).
2. Sima Qian, Approximately 145 BC–approximately 86 BC. Historical records. Dawson, Oxford University Press. ISBN 0192831151. OCLC 28799204.
3. Jadasz, Janusz et al., “The remyelination Philosopher's Stone: Stem and progenitor cell therapies for multiple sclerosis”, Cell and Tissue Research, vol. 349.1, 2012, pp. 331–347.
4. Kontis et al., “Future life expectancy in 35 industrialized countries: Projections with a Bayesian model ensemble”, The Lancet, vol. 389.10076, 2017, pp. 1323–1335.
5. “Dementia”, World Health Organization, 19 September 2019: https://www.who.int/news-room/fact-sheets/detail/dementia (link as of 2/12/19).
6. Wimo et al., “The worldwide costs of dementia 2015 and comparisons with 2010”, Alzheimer's & Dementia, vol. 13.1 2017, pp. 1–7.
7. Ikegami et al., “Japanese universal health coverage: Evolution, achievements and challenges”, The Lancet, vol. 378.9796, 2011, pp. 1106–1115.
8. “Smartphone usage in Japan is growing, but feature phones aren’t going away”, eMarketer, 9 May 2018: https://www.emarketer.com/content/smartphone-usage-in-japan-is-growing-but-feature-phones-aren-t-going-away (link as of 2/12/19).
9. Framework for FDA's Real-World Evidence Program, US Food and Drug Administration, December 2018.
10. “Classification of digital health interventions v1.0: A shared language to describe the uses of digital technology for health”, World Health Organization, 2018: https://www.who.int/reproductivehealth/publications/mhealth/classification-digital-health-interventions/en/ (link as of 2/12/19).
11. “WHO Guideline: Recommendations on digital interventions for health system strengthening”, World Health Organization, 2019: https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/ (link as of 2/12/19).
12. “Health and healthcare in the Fourth Industrial Revolution: Global Future Council on the future of health and healthcare 2016-2018”, World Economic Forum, May 2018: https://www.weforum.org/reports/health-and-healthcare-in-the-fourth-industrial-revolution-global-future-council-on-the-future-of-health-and-healthcare-2016-2018 (link as of 1/10/19).
13. Borgman, Big Data, Little Data, No Data: Scholarship in the Networked World, MIT press, 2015.
14. Galloway, The Four: TheHhidden DNA of Amazon, Apple, Facebook and Google, Portfolio, 2017.
15. Solove, “Introduction: Privacy self-management and the consent dilemma”, Harvard Literary Review, vol. 126, 2012, pp. 1880–1903.
16. Okamoto, “Challenges of disaster countermeasures and the utilization of personal information – policy developments indicated by the Disaster Countermeasures Basic Act and the Consumer Safety Act” [Translated from Japanese], Social Informatics, vol. 3 3, 2015, pp. 1–14.
17. “No progress in confirming the safety of disabled people. The Personal Information Protection Law is a stumbling block” [translated from Japanese], Yomiuri, 4 June 2011.
18. “Disaster victims of the Great East Japan Earthquake – What is behind the high mortality rate? Interim summary of JDF support activities and recommendations” [Unfinished manuscript translated from Japanese]; Second study meeting on evacuation support for people requiring assistance during a disaster: http://www.bousai.go.jp/taisaku/hisaisyagyousei/youengosya/h24_kentoukai/2/6_1.pdf (link as of 2/12/19)
19. “Guidelines on consent under Regulation 2016/679 (wp259rev.01)”, European Commission, 7 June 2018: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (link as of 2/12/19).
20. “Regulation (EU) 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)”, European Commission, 27 April 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679 (link as of 2/12/19).
21. Benoli and Becher, “The duty to read the unreadable”, Boston College Law Review, vol. 60, 11 January 2019.

22. “Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison-shopping service”, European Commission, 27 June 2017: https://europa.eu/rapid/press-release_IP-17-1784_en.htm (link as of 2/12/19).

23. Storbeck and Murgia, “Germany blocks Facebook from pooling user data without consent”, Financial Times, 7 February 2019: https://www.ft.com/content/3a0351b6-2ab9-11e9-88a4-c32129756dd8 (link as of 2/12/19).

24. “METI releases draft interim report of the Study Group on the Improvement of the Trade Environment Involving Digital Platform Businesses”, Ministry of Economy, Trade and Industry (Japan), 5 November 2018: https://www.meti.go.jp/english/press/2018/1105_003.html (link as of 2/12/19).

25. “Proposal of the Anti-Monopoly Act concerning the abuse of a dominant position in transactions between digital platform players and consumers providing personal information” [Translated from Japanese], Japan Fair Trade Commission, 29 August 2019: https://www.jftc.go.jp/houdou/pressrelease/2019/aug/190829_dpfpc2.pdf (link as of 2/12/19).

26. “23USTR announces initiation of Section 301 investigation into France’s Digital Services Tax”, The United States Trade Representative,10 July 2019: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/july/ustr-announces-initiation-section-301 (link as of 2/12/19).

27. “24EUR-Lex, Regulation (EU) 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)”: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 (link as of 2/12/19).

28. “European Data Protection Board”, ePrivacy Regulation, 2019: https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_en (link as of 2/12/19).

29. “NIST Privacy Framework: A tool for improving privacy through enterprise risk management”, National Institute of Standards and Technology, September 2019: www.nist.gov/privacy-framework (link as of 5/12/19).

30. California Consumer Privacy Act, 2018: http://www.caprivacy.org (link as of 2/12/19).

31. “Cross-border data flows: Where are the barriers, and what do they cost?”, Information Technology and Innovation Foundation, May 2017: https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost (link as of 1/11/2019).

32. The APEC Cross-Border Privacy Rules (CBPR) System: http://cbprs.org (link as of 1/11/2019).

33. “Comprehensive and Progressive Agreement for Trans-Pacific Partnership”, New Zealand Ministry of Foreign Affairs and Trade: https://www.mfat.govt.nz/en/about-us/who-we-are/treaties/cptpp (link as of 1/11/2019).

34. “G20 Osaka Leaders’ Declaration”, Ministry of Foreign Affairs of Japan, 28–29 June 2019: https://www.mofa.go.jp/ecm/ec/page22e_000895.html (link as of 1/10/2019).

35. MyData: https://mydata.org (link as of 2/12/19).

36. Blue Button: https://www.healthit.gov/topic/health-it-initiatives/blue-button (link as of 2/12/19).

37. Janeček, “Ownership of personal data in the internet of things, computer law and security review”: https://doi.org/10.1016/j.clsr.2018.04.007 (link as of 2/12/19).

38. The Open Data Foundation: http://www.opendatafoundation.org (link as of 2/12/19).

39. “The FAIR data principles”, Force11: https://www.force11.org/group/fairgroup/fairprinciples (link as of 2/12/19).

40. Beauchamp, Principles of Biomedical Ethics, 5th ed., Oxford University Press, 2001.

41. “Data policy in the Fourth Industrial Revolution”, The Ministry of Cabinet Affairs and the Future, United Arab Emirates and the World Economic Forum, May 2018: https://www.weforum.org/whitepapers/data-policy-in-the-fourth-industrial-revolution-insights-on-personal-data (link as of 1/10/19).

42. Sen, “Elements of a theory of human rights”, Philosophy and Public Affairs, Fall 2004.

43. Dworkin, Taking Rights Seriously, Harvard University Press, 1977.

44. “Regulation (EU) 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)”, European Commission, 27 April 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679 (link as of 2/12/19).

45. Kaye et al., “Dynamic consent: a patient interface for 21st-century research networks”, European Journal of Human Genetics, 23 (2), February 2015, pp. 141–146.

46. Waldman, Privacy as Trust: Information Privacy for an Information Age”, Cambridge University Press, March 2018.

47. Richards and Solove, “Privacy’s other path: Recovering the law of confidentiality,” Georgetown Law Journal, 96, 2007, pp. 123, 156–158, 182.

48. Cavoukian, “Privacy by design: The seven foundational principles implementation and mapping of fair information practices”, 2009: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (link as of 2/12/19).

49. “Preliminary draft of privacy framework”, National Institute of Standards and Technology, 6 September 2019: https://www.nist.gov/privacy-framework/working-drafts (link as of 2/12/19).

50. “How do we apply legitimate interests in practice?”, Information Commissioner’s Office LIA (Legitimate Interest Assessment): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice (link as of 2/12/19).

51. “Towards the construction of next generation healthcare system utilizing ICT” [Japanese], Ministry of Health, Labour and Welfare, 19 October 2016: https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000140306.pdf (link as of 2/12/19).

52. “Secondary use of health and social data”, Ministry of Social Affairs and Health, Finland: https://stm.fi/en/secondary-use-of-health-and-social-data (link as of 2/12/19).

53. “Act on anonymously processed medical information to contribute to medical research and development”, Ministry of Justice: http://www.japaneselawtranslation.go.jp/law/detail/?id=3343&vm=04&re=01&new=1 (link as of 2/12/19).

54. “The Sustainable Development Goals report 2018”, United Nations, 20 June 2018: https://www.un.org/development/desa/publications/the-sustainable-development-goals-report-2018.html (link as of 2/12/19).

55. “Universal Health Coverage”, World Health Organization: https://www.who.int/westernpacific/our-work/universal-health-coverage (link as of 2/12/19).

56. Mill, On Liberty, 8th ed., Hackett Publishing Company, 1978.

57. Dworkin, Paternalism, Morality and the Law, Wadsworth Publishing, 1971.

58. Feinberg, “Legal paternalism”, The Canadian Journal of Philosophy, vol. 1, no. 1.

59. GDPR Section 4; “Right to object and automated individual decision-making”, Article 21; “Right to object”, Article 22; “Automated individual decision-making, including profiling”.

60. GDPR Article 6; “Lawfulness of processing”.

61. Act on the Protection of Personal Information (Japan), 2003, Article 23; paragraph 1(3)–(4).

62. Patent Act (Japan), 1959, Article 83; paragraph 1–2.

63. Emanuel et al., “What makes clinical research in developing countries ethical? The benchmarks of ethical research”, The Journal of Infectious Diseases, 2004, vol. 189, no.5, p. 930.

64. “WHO Framework Convention on Tobacco Control”, World Health Organization: https://www.who.int/fctc/text_download/en/ (link as of 2/12/19).

65. Ferguson, “Lessig on privacy: Economics, technology will drive data retention practices”, CLMP: https://www.thewisemarketer.com/headlines/lessig-on-privacy-economics-technology-will-drive-data-retention-practices (link as of 2/12/19).

66. Law to revise a part of the Health Insurance Act, etc. for the proper and efficient operation of the medical insurance system.

67. Sunstein. “Choosing not to choose”, Duke Law Journal, vol. 64, 2014, p. 1.

68. Raz, “Authority and justification”, Philosophy and Public Affairs, vol. 14, 1985, pp. 3–29.

69. Raz, Practical Reason and Norms, 2nd ed., Princeton University Press, 1990, pp. 35–48.

70. Marmor, Interpretation and Legal Theory, Oxford University Press, 1992.

71. Rawls, Justice as Fairness: A Restatement, Harvard University Press, 2001.

72. Waldron, The Dignity of Legislation, Cambridge University Press, 1999.

73. Rocher et al., “Estimating the success of re-identifications in incomplete datasets using generative models”, Nature Communications, 10. 10.1038/s41467-019-10933-3, 2019.

74. “MOH to introduce measures to reduce sugar intake from pre-packaged sugar-sweetened beverages”, Ministry of Health, Singapore, 10 October 2019: https://www.moh.gov.sg/news-highlights/details/moh-to-introduce-measures-to-reduce-sugar-intake-from-pre-packaged-sugar-sweetened-beverages (link as of 1/10/19).

75. “Relevant ministerial conference on child abuse prevention measures, emergency comprehensive measures for strengthening child abuse prevention measures”, Ministry of Health, Labour and Welfare (Japan), 20 July 2018, https://www.mhlw.go.jp/content/11900000/000335930.pdf (link as of 2/12/19).

76. “Publication of survey results about missing people including those with dementia” [Translated from Japanese], Ministry of Health, Labour and Welfare, 19 September 2014: https://www.mhlw.go.jp/stf/houdou/0000058648.html (link as of 2/12/19).

77. Shibasaki, “Issues of support for family caregivers in the integrated community care system: Study on municipal insured long-term care service plans” [Japanese], 2017: https://rikkyo.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=15551&item_no=1&page_id=13&block_id=49 (link as of 2/12/19).

78. “Data collaboration for the common good”, World Economic Forum and McKinsey & Company, April 2019: https://www.weforum.org/reports/data-collaboration-for-the-common-good-enabling-trust-and-innovation-through-public-private-partnerships (link as of 1/10/19).

79. Kee and Forrer, “Private finance initiative: The theory behind the practice”: www.researchgate.net/publication/228971408_Private_Finance_Initiative-The_Theory_Behind_Practice (link as of 5/12/19).

80. Waldron, The Dignity of Legislation.

81. “Value in healthcare”, World Economic Forum and Boston Consulting Group (BCG), December 2018: https://www.weforum.org/reports/value-in-healthcare-accelerating-the-pace-of-health-system-transformation (link as of 1/10/19).

82. “Undiagnosed Diseases Program”, National Human Genome Research Institute: https://www.genome.gov/Current-NHGRI-Clinical-Studies/Undiagnosed-Diseases-Program-UDN (link as of 2/12/19).

83. “The initiative on rare and undiagnosed disease (IRUD)”, Japan Agency for Medical Research and Development: https://www.amed.go.jp/en/program/IRUD (link as of 2/12/19).

84. Matchmaker Exchange: https://www.matchmakerexchange.org (link as of 2/12/19).

85. Dyke, Linden et al., “Registered access: authorizing data access”, European Journal of Human Genetics, vol. 26, no. 12, December 2018, pp. 1721–1731. doi:10.1038/s41431-018-0219-y. PMID: 30069064; PMCID: PMC6244209.

86. “Policies on release of human genomic sequence data Bermuda-quality sequence”, US Department of Energy, 1997: https://web.ornl.gov/sci/techresources/Human_Genome/research/bermuda.shtml (link as of 1/10/19).

87. Rossi, “How the Snowden revelations saved the EU General Data Protection Regulation”, The International Spectator, Italian Journal of International Affairs, vol. 53, no. 4, November 2018 , pp. 95–111, doi: 10.1080/03932729.2018.1532705.

88. Mettler, “Blockchain technology in healthcare: The revolution starts here”, 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016, pp. 1–3.

89. Ballout, Al-Shorbaji, Abu-Kishk et al., “UNRWA’s innovative e-Health for 5 million Palestine refugees in the Near East”, BMJ Innovations, vol. 4, 2018, pp. 128–134.

90. “Connected health: Empowering health through interoperability”, Global Digital Health Partnership (GDHP): https://www.gdhp.org/media-hub/news_feed/gdhp-reports (link as of 1/11/2019).

91. Berlin, Four Essays on Liberty, Oxford University Press,1969.

92. Nozick, Anarchy, State and Utopia, Basic Books, 1974.

93. Rawls, The Law of Peoples with the Idea of Public Reason Revisited, Harvard University Press, 1999.

94. Nietzsche, On the Genealogy of Morality: A Polemic, 1887: https://archive.org/details/genealogyofmoral00nietuoft/page/n6 (link as of 1/11/2019)

95. “The Sustainable Development Goals report 2018”, United Nations, 20 June 2018: https://www.un.org/development/desa/publications/the-sustainable-development-goals-report-2018.html (link as of 2/12/19).

96. “Globalization 4.0”, World Economic Forum, April 2019: https://www.weforum.org/whitepapers/globalization-4-0-shaping-a-new-global-architecture-in-the-age-of-the-fourth-industrial-revolution (link as of 1/10/19).

97. “Federated data systems: Balancing innovation and trust in the use of sensitive data”, World Economic Forum, 16 October 2019: https://www.weforum.org/whitepapers/federated-data-systems-balancing-innovation-and-trust-in-the-use-of-sensitive-data (link as of 1/11/19).

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org