Chapter Nine: Data Localization: Policymaking or Gambling?

Nikita Melashchenko[[1]](#footnote-1)\*

‘Sir, the possibility of successfully navigating an asteroid field is approximately 3,720 to 1.’

C-3PO, Star Wars: The Empire Strikes Back

# Abstract

The benefits of the information society come at the price of increasing data dependency. This creates tensions between economic, privacy, and public security interests. While data fuels the digital economy and production of cross-border value, it also affects power relations between states and other actors. In response, data localization policies have emerged addressing data flows in the context of information sovereignty. This chapter unfolds the basic concept of data localization and outlines how the underlying policy objectives correspond within the WTO framework. It further examines the principles of data regulation drawing on the nature of information and its lifecycles. The chapter concludes with a mapping tool for data localization policies and moves towards the analytical framework for data regulation.

# Introduction

Data has a location and its regulation matters. Whether data constitutes paper records collecting dust on a shelf, or electronic records embedded in a database, it is physically stored somewhere. In a data dependent society, the governance of data and specifically its physical infrastructure is critically important as they are the basis of all activities, particularly which take place in virtual reality. No services provided in cyberspace (e.g. messengers, online video games or cloud storage) can work without servers maintained in the real world.

However, the whole architecture of storing data while providing services is invisible to users and is therefore seen as a technical matter.[[2]](#footnote-2) Nonetheless, depending on the regulatory model, physical infrastructure might affect social welfare in one way or another. This is evident in the emerging fight for allocation and redistribution of data among storage facilities in various jurisdictions. One of the tools states use in this struggle is data localization (DL) – the reason why LinkedIn stopped operating in Russia, Apple is opening data centers in China and moving encryption keys onshore, and Microsoft wallowed in disputes with the US Government.[[3]](#footnote-3)

States have been utilizing the localization of technology and information as a policy tool for years.[[4]](#footnote-4) When states adopted privacy and data protection regulations in the 1970s, scholars began analyzing the possibility of data privacy and international laws colliding.[[5]](#footnote-5) The discussion eventually recognized important international trade issues: data is foundational to most business interactions, meaning that limiting data flows directly affects trade.[[6]](#footnote-6) However, little attention has been paid to the variety of DL regulations and how such variety affects the end results of regulatory policies.

To keep up with the social and business expectations and practices the DL discussion has to transform.[[7]](#footnote-7) Designing smart data regulations and calibrating DL is necessary given the dependency of the global community on data. However, this is impossible unless we consider the diverse kinds of information and the different regulatory goals that states seek to achieve through controlling information. Thus, DL is not a single, uniform policy measure that always has the same positive or negative consequences; it all depends on what DL measure is adopted. If regulators fail to make DL measures that are fair and just, they risk causing conflict, whether at domestic or international levels.

This chapter explains the essence of DL policies, including the basic goals they seek to achieve. It reviews DL policy taxonomies and explains their limitations. Then, it outlines the tensions between privacy, information sovereignty and international trade in the context of the World Trade Organization (WTO). Against this background, it examines the role of information management cycles (IMCs) and regulatory principles in data regulation. This allows the final analysis that maps DL policies and provides insights into how DL features such as storage location and technological implementation could affect the output of DL policy – providing the key analytical framework for crafting data regulations that avoid negative consequences. While mapping is not a new theory, it is the analytical framework that should initiate the transition from DL taxonomical description to data policy evaluation, modelling and projection.

# What is Data Localization?

The term *data localization* refers to compulsory legal requirements to store data in a specific territory. This broad concept is implemented in a myriad of laws and regulations.[[8]](#footnote-8)

DL policy aims to achieve multiple social goals and potentially may disrupt the informational environment, where agents interact and contribute to improvement of social welfare.[[9]](#footnote-9) This is due to conceptual labyrinth where states are forced to regulate the use of technologies that facilitate universal human rights, promote economic activities and enhance national security, despite the way that these values can come into conflict. Encrypted apps such as Telegram and Zello are the examples of technological progress reaching twofold results. On one hand, they protect privacy and globally improve welfare; on the other they raise national security issues by limiting opportunities to enforce domestic legislation regarding users and their own activities.[[10]](#footnote-10)

DL practices continuously evolve and have drawn wide attention of scholars in the last few years. There have been several taxonomies of DL practices that are substantively different, but similar in descriptive approach.[[11]](#footnote-11) Broad measures embrace as much data as possible, while narrow DL measures can specify particular sets of data or particular businesses that are obliged to localize data.[[12]](#footnote-12) On a broad approach DL measures could be defined as any measures that affect cross-border data transfer. Further, they could be grouped by the forms of implementation: (i) rules prohibiting overseas data transfers; (ii) rules restricting overseas data transfers by authorization; (iii) rules requiring *per se* localization of data; (iv) taxes on data export.[[13]](#footnote-13) Such classification is not exhaustive. It could be supplemented at least with two additional types of DL: (v) disclosure of cryptographic keys; and (vi) obligatory disclosure of the requested information by entities subject to a particular jurisdiction regardless of the storage location.[[14]](#footnote-14) Relying on the broad approach scholars also distinguish two more categories of DL measures by distinguishing between different technological means of implementation. Thus, states invoke policies of localized data hosting (e.g. sole or local copy) and localized data routing (e.g. data packets routing through the designated routes).[[15]](#footnote-15) Such state interventions in data traffic are usually ensured by cooperation with internet service providers such as content filtering (censorship), access control (website blocking) and regulation of privacy enhancing technologies such as virtual private networks.[[16]](#footnote-16) On the narrow approach to DL, there are three types of DL measures: (i) requirements to store *all* data in facilities located inside of the state; (ii) requirements to store *specific* sets of data in facilities located inside of the state; and (iii) requirements to transfer data only to states with adequate legislative and security measures in place with particular purposes and for a limited time.[[17]](#footnote-17)

Whatever particular DL measures are taken, they may be seen as information barriers,[[18]](#footnote-18) as they can limit information flows in various ways within the infosphere or specifically within a particular political agent like a state or economic union.[[19]](#footnote-19) DL makes access to localized data harder for some agents and increases the informational gap between them, while strengthening privacy and information sovereignty protection. However, DL is not only about building informational walls to exclude access of external agents, because the data also becomes more accessible for agents in the jurisdiction to which it is localized. Hence, DL can be a tool for preventing or facilitating access to information, depending on how it is used.

Before proceeding to examine and evaluate possible DL outcomes, it will be necessary to understand the legal and policy problems that arise from the tension between the three concepts that provided grounds for DL in the first place.

# Localization Tensions: Privacy – Data Sovereignty – International Trade

DL raises theoretical and practical issues on many levels. First, there is the issue of individual privacy, in particular the desire to protect personal (identifiable) information (PII) from others. Privacy over PII is the ability ‘to determine […] when, how, and to what extent information about […] [*individuals, groups, institutions*] is communicated to others’.[[20]](#footnote-20) Second, states as independent agents interact with individuals as well as other states. They also have an interest in protecting and accessing information that has value to them. Thus, a notion of data sovereignty arises, which in fact is very similar to individuals’ privacy in terms of guarding data of a critical importance by an independent agent. Finally, DL policy affects the free use of information in markets including cross-border trade, where an agenda to liberalize trade by reducing restrictions on imports and exports prevails.

These layers are inter-dependent. Privacy determines not only personal security, but also state security (e.g. consider a Twitter bot that is tracking movements of top public officials,[[21]](#footnote-21) a fitness app exposing military bases,[[22]](#footnote-22) a security breach exposing records of active military).[[23]](#footnote-23) In turn, data sovereignty provides both individual and institutional data protection (e.g. in 2007 the government of Estonia had to cut off the country from the outside internet in order to stop a cyber-attack and prevent possible data loss).[[24]](#footnote-24) International trade therefore has an interface with domestic and international regulation of privacy as well as rules regarding the use of state information (e.g. requirements established for activities related to critical information infrastructure).[[25]](#footnote-25)

Consequently, problems arise where information restrictions provided by the first two layers start to compete between each other and conflict with international obligations established by the third. In particular, the WTO covered agreements[[26]](#footnote-26) establish the most inclusive liberalized trade regime in the world by requiring non-discrimination and predictable market access.[[27]](#footnote-27) Nonetheless, WTO members frequently restrict non-discrimination obligations and market access for foreign goods and services and this includes restrictions on data flows.[[28]](#footnote-28) Under trade rules, DL measures might constitute a type of non-tariff barrier in digital trade, which might affect trade in services, goods and intellectual property (IP) or constitute a technical barrier to trade. However, none of the legal issues raised by DL implementation have been tested before the WTO dispute resolution body, and therefore the application of the WTO rules (about which there are different interpretations in existing disputes) remains a matter of debate.[[29]](#footnote-29)

In theory the WTO regime should provide certainty and predictability of international trade, but currently it does not do so in relation to data flows. Data usage falls under numerous legal categories and the WTO Agreement provides various exceptions for legitimate non-compliance to achieve goals such as the protection of individuals’ privacy.[[30]](#footnote-30) Such protection has to be related to PII processing and dissemination. Another exception is focused on states’ safety, which in turn can mean many things. There is also a general exception concerning public order, which applies in the event of a ‘genuine and sufficiently serious threat to important societal values’.[[31]](#footnote-31) Finally, states could purport to rely on a security exception which permits to impose any measures that they consider necessary in time of emergency in international relations. States with DL regulation may claim any of these broad exceptions as justification for protecting data sovereignty. Although these matters (particularly, the DL measure’s necessity to achieve the goal) arise under the WTO regime and therefore they should be resolved accordingly by means of treaties interpretation and their application to particular facts, one inevitably will face a dilemma of weighing importance of societal values.

In assessing various state DL measures’ compliance with WTO obligations, one will ask the following long-standing questions. Is privacy more important than national security? Is it vice versa? Should cross-border data flows be enforced to ensure international trade in any event at the expense of these values? How does one determine the balance between several societal values? How should regulatory practices look to reach and preserve such a balance? In the end of the day, do DL measures serve data justice within a complex multi-agent system? Do they amount to smart and fair data regulation? These kinds of questions cannot and should not be answered solely in context of the existing law.[[32]](#footnote-32) Consequently, we should look beyond that to other approaches that may provide guidance.

# Regulating Information Management Cycles

Rapid datafication consisting of data computerization and reevaluation has sparked the discussion of data power and its connection to social justice.[[33]](#footnote-33) This gave rise to the idea of data justice – an ethical guide for information society and the basis of data regulation. Data justice being a fairly new phenomenon is the subject of research within various fields of study.[[34]](#footnote-34) The notion of data justice reflects on data governance and its effects on social and economic justice. Data justice in the context of DL policing highlights the role of data within the tripartite power relations between individuals, states and international institutions explained above. In other words, data justice is the pursuit of fair data use by agents aimed at corporate and state surveillance, privacy protection and free data flows for the purpose of economic and technological development. This chapter posits that data justice and hence smart data regulation analysis should take into account the variety of regulatory institutions concerning data such as PII and IP in all their numerous forms, and efficient information lifecycle management consisting of generation, collection, storage, processing, distribution, usage, and erasure as a coherent system because the regulatory system is the foundation of any kind of justice and contemporary society is not only driven by information but also depends on it to function properly.[[35]](#footnote-35)

Current research has been limited by the binary constraints of traditional regulatory approaches that currently characterize the discussion of the balance between private and public interests regarding the treatment of IMCs (i.e. ensuring data justice). This prevents the elaboration of satisfactory solutions that can maintain complex multi-level systems such as DL. Hence, it is necessary to overcome such limitations.

Conceptually it is reasonable to assume that, depending on the particular structure of a DL policy, a measure could serve one or more policy goals by countless means. At the same time, such means should be analyzed as whole since one small detail could determine the output of the system. For instance, would a measure fully depriving individuals of their autonomy to guard data serve the purpose of privacy protection? How does a DL system technically incapable of enforcing a law – or prone to over-enforcement – contribute to serving data justice and account for necessity? Mapping DL practices should help answer these questions.

Any data regulatory practice should be evaluated on the basis of how it affects the well-being of agents and the informational environment. Any decrease in size or corrosion of quality of information will cause the infosphere to shrink in terms of content, forms and patterns.[[36]](#footnote-36) This leads to fewer opportunities for agents to beneficially interact and thus to contribute to welfare. Hence, the more restrictive DL policy, the higher the deficit of information and the less space for agents to communicate. However, it does not mean that information processes should not be regulated at all. Clearly, such values as privacy, national security and trade are all important. There have always been certain types of data and information processes that states rigorously restricted on domestic and international levels for the benefit of all agents. But what matters is how states give effect to restrictive information policies and what the overall output of such regulatory system is.[[37]](#footnote-37)

General regulatory principles such as consistency, certainty, effective implementation, stability, minimization of costs and market distortions, compatibility with trade facilitation and others are meant to provide regulators with the framework under which states are more likely to come up with a better output for the society.[[38]](#footnote-38) Thus, no society needs a regulatory mechanism (e.g. regarding theft) that is inconsistent and impossible to implement because the effect of such regulation tends to zero, resulting in more risks for the society.

In the context of data, that would mean an unjustified and unnecessary fracture of the IMCs. Consider the following example. IP is information identified as a specific category of information, the control of which is treated by the society in a special way. The Berne Convention provides regulation for literary works and covers the whole IMC.[[39]](#footnote-39) For instance, creation and record are governed by the norms regarding the form of literary works, publication and formalities (Articles 2, 3, 5); processing and collection are resembled in provisions regarding derivative works (Article 2); distribution is covered by rules on reproduction (Article 9); provisions concerning use without charge regulate information consumption (Article 10); erasure is envisaged by prescribed moral rights (Article 6*bis*). By over- or non-regulation of a particular section of the literary work management cycle, the regulator could break it, eventually resulting in the underproduction of literary works. This negative effect on generation, dissemination and consumption of information consequently would affect the state of welfare.[[40]](#footnote-40)

This system also demonstrates tensions between private and public monopoly over information and international obligations. Rephrasing our previously introduced traditional definition of privacy, we might say that the ‘right to exclude others’ in IP is the right to determine when, how, and to what extent information *created* by individuals, groups or institutions is communicated to others. States have their own interests regarding information flows of the category *literary works* and the Berne Convention provides them with a possibility of legitimate non-compliance by the right of censorship (Article 17). However, as the Berne Convention is a unification act and therefore relies on states’ regulatory autonomy and modus of creativity, states independently decide on how they are going to construct their censorship policy, what constitutes necessity, to what extent they are willing to sacrifice regulatory principles in order to reach their objectives. Inevitably, some regulatory practices will appear better than others.

The same structure applies to DL measures dealing with storage location and processing of information (which in fact in many cases includes not only PII, but other categories of information such as IP) that might result in data injustices and disrupt information lifecycles, thus making them inefficient. General regulatory principles aimed at maximizing win-win regulatory end results could therefore provide a threshold against which it would be possible to compare DL models. The following section is dedicated to informational construction of DL and evaluation of regulatory practices.

# Mapping Data Localization Regulatory Practices

DL could be dynamically modelled depending on the chosen regulatory tools (variables) and their subject matter (types), which in turn constitute each of the policy goals (observables) (Figure 1). Each sequence of typed variables uniquely determines the subject matter of observables and therefore the output of the DL policy.[[41]](#footnote-41) Such output in terms of welfare consequences then could be measured against regulatory principles.

*Figure 1.*

Depending on collection of variables, their types and interpretation it is possible to construct many variants of DL systems. For instance, *category* variable determines the scope and thus differently characterizes observables. Thus, localization of governmental data should affect the correlation of privacy, sovereignty and trade differently compared to localization of undefined categories of PII. The broader the scope, the more it attributes to the protection of privacy and data sovereignty because data subjects and states acquire more effective control over data as it is physically available to them. However, it becomes more burdensome for international trade and domestic market actors as their economic costs rise as well as more restrictive on individual liberties because the autonomy to decide the fate of data shrinks.

Moreover, this relationship depends on the legal form and meaning of the *types*. For instance, in terms of categories Russia requires the localization of (i) PII and (ii) communications, while Australia requires the localization of (iii) personally controlled electronic health records (PCEHR).[[42]](#footnote-42) The reason why researchers classify (i) and (ii) as broad and (iii) as narrow is that they differ in scope and hence the amount of data required to localize. In Russia PII means any information that can identify a person. Communications in turn include metadata and content data or any information transmitted/received by user over the internet/other means of telecommunications.[[43]](#footnote-43) On the other hand, PCEHR constitutes information about and connected to the customer, which is related to health and recorded in a special system or register. Obviously, the scope differs considerably depending on the attributes *any, transmitted,* and *related to health*. The broader the meaning of a category the more policy space a state acquires in the course of sovereignty protection. However, it creates uncertainty for individuals and international market participants that might result in an overall disadvantage.

Although, this system is not static and the output changes if other variables are introduced. Thus, for (i) regulated agents include any persons that are involved in PII management cycle at any stage and specific entities that ensure communications regarding measure (ii). For measure (iii), regulated agents are envisaged in the closed list of entities that are authorized to work with PCEHR. Again, these attributes make the scope narrower or broader. Further, all measures contain a non-finite amount of information formats and mediums (e.g. personal and public records, health records, audio, video, etc.). This attribute broadens the definition of data for all compared measures.

Such variables as location and method of storage also greatly affect the output. In case DL mechanism prescribes storage of data in a particular region or even in a particular datacenter, it creates and worsens to a degree the so-called jackpot and protected local provider (PLP) problems.[[44]](#footnote-44) It is one thing to prescribe storage within a particular territory thus limiting the market by territory, technical capabilities and competition, and another if a regulator specifies authorized market players thus limiting the environment even more. In this regard even forms of ownership (e.g. public or private) should play a crucial role, since owners of datacenters and their numbers determine the market.

The enforcement framework matters as well. DL measures are usually enforced by common regimes of legal sanctions or technical enforcement such as blocking schemes that preclude service providers from operating on a particular territory. Just as the wording of a statute makes a difference in the course of its application, technical characteristics of the blocking scheme determine the output of a DL measure. For example, in many instances DL in Russia is based on blocking IP addresses, while DL in New Zealand is based on blocking of a combination of IP and URL addresses. Both methods provide different outputs. While the former is easier and cheaper (this is relevant for those who pay for such enforcement, e.g. state or internet providers) to implement, it blocks every resource that is assigned to a blocked IP address, hence resulting in over-enforcement. The latter on the other hand allows the conducting of additional filtering by URL and provides for a precision-guided enforcement mechanism.[[45]](#footnote-45)

It is important to note that the legal bases for invoking such technical enforcement are also of a great significance. For example, it is reasonable to assume that judicial review might reduce possible negative effects of technical enforcement, particularly regarding IP-based mass blocking, more effectively if compared to administrative review. On top of that, the efficiency of these features depends on the meta framework – the rule of law. Regardless of how legal and technological enforcement is formally constructed, in the absence of the rule of law no mechanism would work properly. This applies to the construction of any regulation.

The same rationale applies to a feature of localization of encryption keys, which could be achieved by various means such as compulsory assistance, lawful hacking and prior design of backdoors.[[46]](#footnote-46) Each method has its own advantages and disadvantages but once again it is crucial to emphasize the importance of legal and technical implementation frameworks. For instance, compulsory assistance that implies sending encryption keys over unsecured means of communication is not better than lawful hacking against an undefined set of persons without any form of legal review.[[47]](#footnote-47)

Hence, there is a plethora of elements that at the end of the day may invoke the law of unintended consequences and turn a DL mechanism intended to regain control over data for the sake of privacy and security into something quite the opposite.[[48]](#footnote-48) It is considerably difficult to argue that a DL scheme consisting of an obligatory centralized governmental data storage regarding broad categories of data and compulsory assistance scheme contributes to privacy protection as this mechanism clearly erodes individuals’ autonomy to determine the fate of their data. Neither does it amount to reasonable standards of security protection as such a model elevates jackpot and PLP problems to a critical level. However, it is only when DL is considered as a complex system should the output be considered because otherwise policymaking turns into gambling.[[49]](#footnote-49)

Based on this could it be reasonably assumed that the Australian measure is *smarter* because it requires the storage of less data? Or could it be concluded that all DL measures are bad regulatory practices just because they establish more burdens? Indeed, either scenario results in the distortion of IMCs. Consequently, DL measures should be constructed as to prevent and remove such distortion by adherence to regulatory principles.

This discussion cannot canvass every link between DL features and regulatory principles. However, the Australian measure, for instance, provides more certainty as it raises less questions about what actually regulated persons ought to store. In contrast, Russian DL measures are very similar to Russian famous ‘yes, no, maybe’, which means a negative reaction of a high uncertainty and possibility to be changed into ‘yes’ and ‘no’ in the future. In other words, it contains a general but not detailed enough meaning, which is contrary to the principle of legal certainty. This is the exact reason why experts cannot even agree on economic consequences because no one knows how much data shall be stored.[[50]](#footnote-50)

Overall, such an approach correlates with the precautionary principle that is familiar to international law including the WTO framework and many legal systems.[[51]](#footnote-51) The precautionary principle has emerged as a response to human activities resulting in environmental degradation and serves as the basis for safeguarding humans’ safety.[[52]](#footnote-52) However, this principle may be applied to regulation of inchoate technologies and therefore IMCs that are constituent to them.[[53]](#footnote-53)

Generally, the precautionary principle aims at preserving conditions critical for humans by eliminating potential negative activities that may alter such conditions even in the absence of a clear and unambiguous causation.[[54]](#footnote-54) Indeed, DL policies look like precautionary measures called to protect states’ data sovereignty and individuals’ privacy. However, under this veil data flows are seen as a potential source of harm and their value (e.g. social, economic, etc.) is often disregarded. Moreover, such one-sided regulatory interventionism allows for trade protectionism only worsening localization tensions explained above. Accordingly, the focus of precautionary protection should also incorporate IMCs which create the operational environment for states, individuals and trade actors.

Finally, uncertainty is the trigger for the precautionary principle.[[55]](#footnote-55) Data flows as well as inchoate technology generate unpredictable events for all the actors of informational environment and therefore sovereignty, privacy and trade. Hence, there is a genuine interest to eliminate uncertainty by introducing precautionary measures. However, the only way to reduce uncertainty is by introducing legal certainty aligned with social expectations which means adherence to the regulatory principles.

By all means, the determination of a threshold of legal certainty regarding IMCs is a nontrivial task. Adopting an approach oriented at IMCs, it is proposed to subject DL policies to the following criteria placed in a hierarchical order:[[56]](#footnote-56)

1. under no circumstances shall a DL policy generate legal uncertainty;
2. a DL policy shall prevent legal uncertainty;
3. a DL policy shall reduce legal uncertainty;
4. a DL policy shall benefit data flows.

The first criterion is of a critical importance and therefore failure to adhere to it would result in over-enforcement. In turn, legal uncertainty exists where a DL policy is inconsistent, disproportionate, technologically and economically unreasonable. For instance, a DL policy introducing a broad localization scheme for undefined data categories, establishing a censorship mechanism at the tremendous cost of private parties that amounts to *carpet website blockings* and on top of that which is arbitrary enforced, would not be justified under the proposed framework in any event. This is due to the fact that it generates legal uncertainty instead of preventing or reducing it. While such a scheme could be highly beneficial for protecting information sovereignty, the generated legal uncertainty would inadequately affect privacy and trade. On the other hand, a DL policy of a high-accuracy that requires law enforcement agencies’ access to communications metadata, regardless of the storage location, with a legally provided possibility to copy such data for security precautions and a blocking scheme, would have higher chances to be justified under the proposed framework. Accordingly, such a DL policy arguably reduces legal uncertainty for all the actors while also benefiting the development of IMCs by eliminating harmful activities. Ultimately, a DL policy requiring the disclosure of software code in the event that such software is exploited for governmental purposes or there is a good reason to believe that a product contains backdoors, which could be used for concealed data collection or result in data breach, also has a better chance to be justified. Respectively, this would be possible because such DL policy would prevent legal uncertainty caused by software products and benefit IMCs by securing confidential data before the event.

As previously described and demonstrated in Figure 1 some features of a DL system might reduce the overall effect of DL, while others worsen its notorious effect. Taking into account the regulatory principles, the more definitive and precise a DL measure is, the more adequate the link between the measure and the policy objective is, the better a possibility to construct a smarter data regulatory regime. Approaching data regulation as a complex system should result in a highly scrutinized regulatory scheme. This might be more effective compared to binary choices.

# Conclusion

Data justice or balance within the framework of power relations over data is obviously necessary in today’s world, but it is impossible to approach without smart data regulation. Far from being a fully designed concept, it is plausible to infer that smart data regulation regarding DL should constitute a small-scaled policy based on an adequate number of regulatory tools (variables) with well-defined subject matter (types) rather than extensive and broad regulation. This is more likely to sustain and enrich IMCs, while ensuring the competing interests of all information agents by means of preserving the balance between legally certain regulatory interventions and private autonomy.

Each detail in a data regulatory mechanism matters. From the overall purpose and wording, to technical nature and implementation. By abstracting elements the regulator risks creating expensive, ineffective and damaging regulations resulting in unintended consequences. The regulator has to be sensitive to every action against information flows and provide safety nets as negligence might result in data injustices and affect societal welfare.

# References

‘Analiz Sushestvujushih Metodov Upravlenija Dostupom K Internet-Resursam I Rekomendatsii Po Ih Primeneniju’, (*Analysis of Existing Methods Regarding Administration of the Access to Internet-Resources and Recommendations on Their Application*). [In Russian]. Official Website of Federal Service for Supervision of Communications, Information Technology and Mass Media, 2013.

Berne Convention for the Protection of Literary and Artistic Works, Sep. 9, 1886, revised at Paris July 24, 1979, 828 U.N.T.S. 221, S. Treaty Doc. No. 99-27, 99th Cong. (1986).

Bossche, Peter van den, and Denise Prevost. *Essentials of WTO Law*, Cambridge: Cambridge University Press, 2016.

Braithwaite, Valerie. ‘Closing the Gap between Regulation and the Community’, in Peter Drahos (ed.), *Regulatory Theory: Foundations and Applications*, Canberra: ANU Press, 2017.

Chander, Anupam, and Uyên P. Lê. ‘Data Nationalism’, *Emory Law Journal* 64.3 (2015).

‘China Cybersecurity Law Update: Finally, Draft Regulations on “Critical Information Infrastructure”’. *Bird & Bird News Centre*, 2017.

Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2713 (2018).

Clark, David D. *Designs for an Internet*. 2017.

‘Data Localization Snapshot’. Information Technology Industry Council. 2017.

Dencik, Lina, Arne Hintz and Jonathan Cable. ‘Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism’, *Big Data & Society* 3.2 (2016): 1–12.

‘Digital Child Exploitation Filtering System’. The New Zealand Department of Internal Affairs, 2009.

Drahos, Peter. *A Philosophy of Intellectual Property*, Aldershot: Ashgate Publishing Company, 1996.

Eger, John M. ‘Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers’, *Law & Policy in International Business* 10.4 (1978): 1055–103.

‘Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions’. EastWest Institute, 2018.

Federal’nyi Zakon RF ob Informacii, informacionnyh tehnologijah i o zashite informacii [Federal law of the Russian Federation on Information, Information technologies and Protection of Information], Rossiiskaia Gazeta, July 31, 2006.

Floridi, Luciano. *The Ethics of Information*, Oxford: Oxford University Press, 2013.

———. ‘The Method of Levels of Abstraction’, *Minds & Machines* 18.3 (2008): 303–29.

GATS: General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

GATT 1994: General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994).

Gervais, Daniel. ‘Regulation of Inchoate Technologies’, *Houston Law Review* 47.3 (2010): 665–705.

Hayes, A. Wallace. ‘The Precautionary Principle’, *Archives Indus. Hygiene & Toxicology* 56 (2005): 161–166.

Kang, Cicilia, and Katie Benner. ‘Russia Requires Apple and Google to Remove Linkedin from Local App Stores.’ *The New York Times*, 6 January 2017.

Kuchler, Hannah. ‘Microsoft Faces Key Ruling in Data Privacy Case.’ *Financial Times*, 17 October 2017.

Kuner, Christopher. ‘Data Nationalism and Its Discontents’, *Emory Law Journal* 64 (2015): 2089–98.

Landler, Mark, and John Markoff. ‘Digital Fears Emerge after Data Siege in Estonia.’ *The New York Times*, 29 May 2007.

Lapowsky, Issie. ‘Voice Chat App Zello Turned a Blind Eye to Jihadis for Years.’ *WIRED*, 16 March 2018.

‘Linkedin to Be Blocked in Russia’. *RAPSI*, 10 November 2016.

Livingston, Scott, and Graham Greenleaf. ‘Data Localisation in China and Other APEC Jurisdictions’, *Privacy Laws & Business International Report* 143 (2016): 22–26.

McMillan, Robert, and Tripp Mickle. ‘Apple to Start Putting Sensitive Encryption Keys in China.’ *Wall Street Journal*, 24 February 2018.

Mozur, Paul, Daisuke Wakabayashi, and Nick Wingfield. ‘Apple Opening Data Center in China to Comply with Cybersecurity Law.’ *The New York Times*, 12 July 2017.

Murdock, Jason. ‘U.S. Marines Email Leak Exposes Secrets of 21,000 Soldiers, Civilians.’ *Newsweek*, 1 March 2018.

‘New Legislation Regulating Cyber Security and the Internet in Russia’. *Clifford Chance Resources*. 2017.

Peng, Shin-yi, and Han-wei Liu. ‘The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?’, *Journal of World Trade* 51.2 (2017): 183–204.

Perez-Pena, Richard and Matthew Rosenberg. ‘Strava Fitness App Can Reveal Military Sites, Analysts Say’. *The New York Times*, 29 January 2018.

‘Principles for Good Governance of Regulators (Public Consultation Draft)’. Organisation for Economic Co-operation and Development, 2013.

‘Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls’. New America, 2018.

‘Russia's “Big Brother Law” to Cost Telecoms $154bln – Report’. *The Moscow Times*. 26 August 2016.

Selby, John. ‘Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?’, *International Journal of Law and Information Technology* 25.3 (2017): 213–32.

Taylor, Linnet. ‘What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally’, *Big Data & Society* 4.2 (2017): 1–14.

‘Telegram Loses Bid to Block Russia from Encryption Keys’. *Bloomberg.* 21 March 2018.

Toor, Amar. ‘This Twitter Bot Is Tracking Dictators' Flights in and out of Geneva’. *The Verge*. 16 October 2016.

‘United States v. Microsoft Corp.’. *SCOTUSblog*. 2017.

‘United States v. Microsoft Corporation (Oral Argument Transcription)’. Supreme Court of the United States. *Official Website*. 2018.

Waters, Richard. ‘Microsoft Setback in Cloud Era Test Case.’ *Financial Times*, 1 August 2014.

———. ‘Microsoft Wins Battle with Us over Data Privacy.’ *Financial Times*, 15 July 2016.

Westin, Alan F. *Privacy and Freedom*, New York: Atheneum, 1967.

‘Work Programme on Electronic Commerce. Removing Cyberspace Trade Barriers: Towards a Digital Trade Environment with Reciprocally Equal Access. Non-Paper from the Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu’. General Council, Council for Trade in Goods, Council for Trade in Services, Council for Trade-Related Aspects of Intellectual Property Rights, Committee on Trade and Development. ‘2018.

WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

1. \* PhD Candidate, Victoria University of Wellington. I wish to thank Professor Susy Frankel and Dr Mark Bennett for suggesting improvements to this chapter. [↑](#footnote-ref-1)
2. World Wide Web and email services based on a client-server model and peer-to-peer applications imply among other things the work of physical components (e.g. processors, storage devices). See David D. Clark, ‘Designs for an Internet’ (2017): pp. 9-11, https://groups.csail.mit.edu/ana/People/DDC/lbook-arch.pdf. [↑](#footnote-ref-2)
3. See ‘LinkedIn to be Blocked in Russia’, *RAPSI*, 10 November 2016, http://www.rapsinews.com/judicial\_news/20161110/277106589.html; Cicilia Kang and Katie Benner, ‘Russia Requires Apple and Google to Remove LinkedIn From Local App Stores’, *The New York Times*, 6 January 2017, https://www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html; Paul Mozur, Daisuke Wakabayashi, and Nick Wingfield, ‘Apple Opening Data Center in China to Comply With Cybersecurity Law’, *The New York Times*, 12 July 2017, https://www.nytimes.com/2017/07/12/business/apple-china-data-center-cybersecurity.html; Robert McMillan and Tripp Mickle, ‘Apple to Start Putting Sensitive Encryption Keys in China’, *Wall Street Journal*, 24 February 2018, https://www.wsj.com/articles/apple-to-start-putting-sensitive-encryption-keys-in-china-1519497574; Richard Waters, ‘Microsoft setback in cloud era test case’, *Financial Times*, 1 August 2014, https://www.ft.com/content/0649c042-18e6-11e4-933e-00144feabdc0; ‘Microsoft wins battle with US over data privacy’, *Financial Times*, 15 July 2016, https://www.ft.com/content/6a3d84ca-49f5-11e6-8d68-72e9211e86ab; Hannah Kuchler, ‘Microsoft faces key ruling in data privacy case’, *Financial Times*, 17 October 2017, https://www.ft.com/content/7d22f1ae-b28d-11e7-a398-73d59db9e399; ‘United States v. Microsoft Corp.’, *SCOTUSblog*, 2017, http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/. [↑](#footnote-ref-3)
4. Consider regulatory institutes such as restrictions on technology export and state secrets. [↑](#footnote-ref-4)
5. For instance, Sweden adopted the Swedish Data Bank Statute as early as 1973. This was a response to the overseas storage of data connected to Swedish citizens. See John M. Eger, ‘Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers’, *Law & Policy in International Business* 10.4 (1978): 1065-81; Christopher Kuner, ‘Data Nationalism and its Discontents’, *Emory Law Journal* 64 (2015): 2091-93; Anupam Chander and Uyên P. Lê, ‘Data Nationalism’, *Emory Law Journal* 64.3 (2015): 713-39. [↑](#footnote-ref-5)
6. At large DL analysis presents taxonomy and being surrounded by countless dichotomies (e.g. data/information, privacy/public security, etc.) was trapped within the binary constraints of traditional regulatory approaches. Justice of the US Supreme Court Anthony M. Kennedy has provided a great example of binary regulatory choices during the oral argument in the *United States v. Microsoft Corporation*. In the course of extraterritoriality discussion Justice Kennedy has raised a question of why should SCOTUS be focused on data location storage v. data location disclosure and whether SCOTUS is forced to make such a choice. See ‘United States v. Microsoft Corporation (Oral Argument Transcription)’, Official Website, (2018), https://www.supremecourt.gov/oral\_arguments/argument\_transcripts/2017/17-2\_j4ek.pdf. [↑](#footnote-ref-6)
7. Valerie Braithwaite, ‘Closing the Gap Between Regulation and the Community’, in Peter Drahos (ed.), *Regulatory Theory: Foundations and Applications* Canberra: ANU Press, 2017, pp. 30-33. [↑](#footnote-ref-7)
8. ‘Data Localization Snapshot (Current as of January 19, 2017)’, Information Technology Industry Council, (2017), https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf. [↑](#footnote-ref-8)
9. On the concept of *infosphere* see Luciano Floridi, *The Ethics of Information*, Oxford: Oxford University Press, 2013, p. 6. [↑](#footnote-ref-9)
10. Issie Lapowsky, ‘Voice Chat App Zello Turned a Blind Eye to Jihadis for Years’, *WIRED*, 16 March 2018, https://www.wired.com/story/zello-app-turned-blind-eye-to-jihadis-for-years/. [↑](#footnote-ref-10)
11. Chander and Lê, ‘Data Nationalism’: 708-13. [↑](#footnote-ref-11)
12. DL measures introduced in Australia (health related data) and Canada (data in possession of public institutions) are examples of a narrow approach. On the contrary, measures adopted by Russia (personal data (PII), communications metadata and content), China (PII and important data collected by ‘network operators’) and Vietnam (data important for national security) fall under a broad approach. See Scott Livingston and Graham Greenleaf, ‘Data Localisation in China and Other APEC Jurisdictions’, *Privacy Laws & Business International Report* 143 (2016): 2-5. [↑](#footnote-ref-12)
13. Chander and Lê, ‘Data Nationalism’: 680. [↑](#footnote-ref-13)
14. See Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2713 (2018); Federal’nyi Zakon RF ob Informacii, informacionnyh tehnologijah i o zashite informacii [Federal law of the Russian Federation on Information, Information technologies and Protection of Information], Rossiiskaia Gazeta, July 31, 2006, item 10.1(4.1). [↑](#footnote-ref-14)
15. Localized data hosting – a requirement to store certain data on servers physically based within the state’s territory. Localized data routing – the requirement to send data packets through servers physically based within the state’s territory. John Selby, ‘Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?’, *International Journal of Law and Information Technology,* 25.3 (2017): 214. [↑](#footnote-ref-15)
16. Content filtering – censorship of data packets based on subject matter or technological requirements. ‘Work Programme on Electronic Commerce. Removing Cyberspace Trade Barriers: Towards a Digital Trade Environment with Reciprocally Equal Access. Non-Paper from the Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu’, Council for Trade in Goods General Council, Council for Trade in Services, Council for Trade-Related Aspects of Intellectual Property Rights, Committee on Trade and Development, JOB/GC/170, JOB/CTG/12 JOB/SERV/277, JOB/IP/29 JOB/DEV/53, 16 February 2018 1, para. 1.3, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/JOBs/GC/170.pdf. [↑](#footnote-ref-16)
17. Shin-yi Peng and Han-wei Liu, ‘The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?’, *Journal of World Trade* 51.2 (2017): 193-94. [↑](#footnote-ref-17)
18. In addition, consider the following examples: data leak prevention systems, rules regarding state secrets, commercial secrets, confidential information, and intellectual property. [↑](#footnote-ref-18)
19. Floridi, *The Ethics of Information,* 232. [↑](#footnote-ref-19)
20. Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967, p. 7. [↑](#footnote-ref-20)
21. Amar Toor, ‘This Twitter Bot is Tracking Dictators’ Flights In and Out of Geneva’, *The Verge*, 16 October 2016, https://www.theverge.com/2016/10/13/13243072/twitter-bot-tracks-dictator-planes-geneva-gva-tracker. [↑](#footnote-ref-21)
22. Richard Perez-Pena and Matthew Rosenberg, ‘Strava Fitness App Can Reveal Military Sites, Analysts Say’, *The New York Times*, 29 January 2018, https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html. [↑](#footnote-ref-22)
23. Jason Murdock, ‘U.S. Marines Email Leak Exposes Secrets of 21,000 Soldiers, Civilians’, *Newsweek*, 1 March 2018, http://www.newsweek.com/us-marines-data-breach-leak-soldier-secrets-hits-21000-soldiers-civilians-825382. [↑](#footnote-ref-23)
24. Mark Landler and John Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’, *The New York Times*, 29 May 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html. [↑](#footnote-ref-24)
25. See Daniel Gervais, ‘Regulation of Inchoate Technologies’, *Houston Law Review* 47.3 (2010): 679-80. Also see ‘New Legislation Regulating Cyber Security and the Internet in Russia’, *Clifford Chance Resources*, 3 March, 2017, https://www.cliffordchance.com/briefings/2017/10/new\_legislation\_regulatingcybersecurityandth.html; ‘China Cybersecurity Law Update: Finally, Draft Regulations on ‘Critical Information Infrastructure’ *Bird & Bird News Centre*, 3 March, 2017, https://www.twobirds.com/en/news/articles/2017/china/draft-regulations-on-critical-information-infrastructure. [↑](#footnote-ref-25)
26. WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994). [↑](#footnote-ref-26)
27. Peter van den Bossche and Denise Prevost, *Essentials of WTO Law*, Cambridge: Cambridge University Press, 2016, pp. 13, 49. [↑](#footnote-ref-27)
28. Ibid, 49. [↑](#footnote-ref-28)
29. E-Commerce WP - Taiwan (2018), 3, para. 3.1. [↑](#footnote-ref-29)
30. GATT 1994: General Agreement on Tariffs and Trade 1994, arts. XX(a), XX(b), XX(d), XXI(b)(iii), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994); GATS: General Agreement on Trade in Services, arts. XIV(a), XIV(c)(ii), XIV(c)(iii), XIVbis(1)(b)(iii), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994). [↑](#footnote-ref-30)
31. GATS, art XIV(a), fn 5. [↑](#footnote-ref-31)
32. Kuner, ‘Data Nationalism and its Discontents’, 2096. [↑](#footnote-ref-32)
33. Lina Dencik, Arne Hintz, and Jonathan Cable, ‘Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism’, *Big Data & Society,* 3.2 (2016): 8-9. [↑](#footnote-ref-33)
34. Linnet Taylor, ‘What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally’, *Big Data & Society,* 4.2 (2017): 1-4. [↑](#footnote-ref-34)
35. Braithwaite, ‘Closing the Gap’, 30-33. [↑](#footnote-ref-35)
36. Floridi, *The Ethics of Information*, 65-67. [↑](#footnote-ref-36)
37. As an alternative to DL policies scholars sometimes refer to the Mutual Legal Assistance Treaties (MLATs). While under MLATs states may agree on information exchange and establish an effective regime of cross-border data interception, this mechanism is extremely time consuming and of a highly political nature. In most cases the request for the information exchange under MLATs may be easily denied. Thus, under the MLAT between Russia and the United States ‘the execution of the request [may be denied if it] would prejudice the security or other essential interests of the Requested Party’. Apparently, the category of essential interests is broad and would have different meanings for both Russia and the United States especially considering the current state of international relations between both actors. Hence, while recognizing the role, although somewhat limited, of MLATs in controlling cross-border data flows, this chapter leaves the question of their potential to constitute a substitute to DL polices open and subject to the future research. See Chander and Lê, ‘Data Nationalism’, 730–735; Peng and Liu, ‘The Legality of Data Residency Requirements’, 201–202; ‘Rethinking Data, Geography, and Jurisdiction: Towards a Common Framework for Harmonizing Global Data Flow Controls’, New America, (2018), 5–8, https://newamerica.org/documents/2084/Rethinking\_Data\_Geography\_Jurisdiction\_2.21.pdf. [↑](#footnote-ref-37)
38. ‘Principles for Good Governance of Regulators (Public Consultation Draft)’, Organisation for Economic Co-operation and Development, (2013), http://www.oecd.org/gov/regulatory-policy/Governance%20of%20Regulators%20FN%202.docx. [↑](#footnote-ref-38)
39. Berne Convention for the Protection of Literary and Artistic Works, Sep. 9, 1886, revised at Paris July 24, 1979, 828 U.N.T.S. 221, S. Treaty Doc. No. 99-27, 99th Cong. (1986). [↑](#footnote-ref-39)
40. Peter Drahos, *A Philosophy of Intellectual Property*, Aldershot: Ashgate Publishing Company, 1996, p. 180. [↑](#footnote-ref-40)
41. See Luciano Floridi, ‘The Method of Levels of Abstraction’, *Minds & Machines,* 18.3 (2008): 305-306. [↑](#footnote-ref-41)
42. ‘Data Localization Snapshot’, www.itic.org. [↑](#footnote-ref-42)
43. Content data – information aimed at the public (e.g. text messages, audio- and video-files). Metadata – data about information aimed at the public (e.g. IP-address and device the content was sent from, time of the content exchange, format of the content). [↑](#footnote-ref-43)
44. Chander and Lê, ‘Data Nationalism’, 716-17. Jackpot problem – a centralized data storage that simplifies access for the intruder (e.g. designating a state-owned data center for an obligatory data storage). Protected local provider problem – a deterioration of local data processing services as a result of a limited competition established by the DL policy (i.e. data processing market shrinks by excluding international businesses). [↑](#footnote-ref-44)
45. ‘Analiz Sushestvujushih Metodov Upravlenija Dostupom k Internet-Resursam i Rekomendatsii po ih Primeneniju’, (*Analysis of Existing Methods Regarding Administration of the Access to Internet-Resources and Recommendations on Their Application*), [in Russian], Official Website of Federal Service for Supervision of Communications, Information Technology and Mass Media, (2013), https://rkn.gov.ru/docs/Analysys\_and\_recommendations\_comments\_fin.pdf; ‘Digital Child Exploitation Filtering System’, The New Zealand Department of Internal Affairs, (2009), http://www.dia.govt.nz/pubforms.nsf/URL/DCESF-PublicInformationPack.pdf/$file/DCESF-PublicInformationPack.pdf. [↑](#footnote-ref-45)
46. ‘Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions’, EastWest Institute, (2018), 32-38, https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf. [↑](#footnote-ref-46)
47. ‘Telegram Loses Bid to Block Russia From Encryption Keys’, *Bloomberg*, 21 March 2018, https://www.bloomberg.com/news/articles/2018-03-20/telegram-loses-bid-to-stop-russia-from-getting-encryption-keys. One of the arguments within discussion of this case was that the Russian Federal Security Service does not provide for a secure means of encryption keys disclosure and allows them to be sent over unsecured mail or email. [↑](#footnote-ref-47)
48. Gervais, ‘Regulation of Inchoate Technologies’, 684-88. [↑](#footnote-ref-48)
49. Consider the following. Russian measures require storing data onshore, but do not prohibit data being transferred abroad in full. Australian measures require storing data onshore by prohibiting any transfer of PCEHR overseas unless redacted, anonymized and conducted by an authorized public agency. Obviously, without taking into consideration other features of the systems it is impossible to conclude whether any of them amount to smart regulatory practice. [↑](#footnote-ref-49)
50. By various estimates only the costs of communications data localisation will be anywhere from $50 million to $154 billion. See ‘Russia's “Big Brother Law” to Cost Telecoms $154Bln – Report’, *The Moscow Times*, 26 August 2016, https://themoscowtimes.com/news/anti-terror-big-brother-law-to-cost-russian-companies-154bln-says-expert-55125. [↑](#footnote-ref-50)
51. See A. Wallace Hayes, ‘The Precautionary Principle’, *Archives Indus. Hygiene & Toxicology* 56 (2005): 161-62. [↑](#footnote-ref-51)
52. Ibid. [↑](#footnote-ref-52)
53. Gervais, ‘Regulation of Inchoate Technologies’, 693-704. [↑](#footnote-ref-53)
54. However, there is a plethora of formulas for the precautionary principle depending on the applicable sector and wording. See Hayes, ‘The Precautionary Principle’, 162. [↑](#footnote-ref-54)
55. Gervais, ‘Regulation of Inchoate Technologies’, 697. [↑](#footnote-ref-55)
56. The proposed framework reflects on the four ethical principles of Information Ethics. See Floridi, *The Ethics of* Information, 70-74. [↑](#footnote-ref-56)