SMU
SINGAPORE MANAGEMENT UNIVERSITY

Centre for
AI and Data Governance

Driving Digital Self-determination[1][2]

Mark Findlay

Background

There is much discussion about how to transit digital self-determination from its conceptual understandings, into action. One important component of the central strategy offered in ‘Creating Trustworthy Data Spaces based on Digital Self-determination’ (the Report) is to offer a voluntary code of conduct to guide the development of trustworthy data spaces. The code of conduct, and the achievement of trustworthy data spaces, the Report asserts, require following basic principles (transparency, control, fairness, responsibility and efficiency. These principles of digital self-determination will in turn represent a governance frame that relies on high standards of stakeholder trust.[3] Even so, the report does not discount other regulatory forces that can influence data spaces and stakeholder trust.

The Report identifies individual and collective components of digital self-determination. In the ‘individual components, it identifies ‘knowledge (understandable, clear and useful), the freedom to make one’s own decisions (about their data) and the *ability to take action. Taking action* is seen as including the possibility to implement one’s decisions in the digital space. Therefore, with principles agreed, and a code of conduct in place, digital self-determination becomes an action strategy – a process that can ensure better opportunities and practices for data management and access in *real-time contexts.*

This note outlines the essentials for an action plan on Digital Self-determination. It takes up from the ‘Recommendations for Action’ in the Report and pivots around establishing safe (trustworthy) data spaces in which digital self-determination can be realized. We make the distinction between safe and trustworthy data spaces, preferring the former as a more encompassing notion. Trustworthiness, while integral to the idea of safety is not the exclusive determinant. Safety can depend on risk reduction, but more so on responsible obligations arising from agreed duties and respectful engagement between duty and obligation.

In ‘Recommendations for Action’ the Report, while recognizing that digital self-determination can be implemented in different ways, prefers to identify various responsibilities for establishing trustworthy data spaces. We concur that DSD cannot progress without or outside safe data spaces. However

[1] This ‘think piece’ was constructed drawing considerably from the fine work in ‘Creating Trustworthy Data Spaces base on Digital Self-determination’ , DETEC & FDFA (30/03/22); and the work of CAIDG on DSD in https://caidg.smu.edu.sg/digital-self-determination

[2] This project is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

[3] The report does not detail this cause and effect. The work on trust from CAIDG offers some guidance - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3857447

essential, context creation is only the first step in an action plan. What follows is the shell for such a plan accepting the importance of principles and orderly conduct, and drawing from the experience of the CAIDG DSD use case on open finance (see appendix for 'outcomes').

Drivers for Digital Self-determination

We have chosen the concept of 'drivers' consciously drawing on the analogy between this action plan and the fact that all computer hardware requires drivers. For the computer, a driver is a set of files that communicates with a computer's operating system to tell the hardware what to do. As we suggest, action plan drivers communicate with the dynamics of DSD to instruct organisations and communities on data control and management. These drivers, therefore, are both communication pathways and operational incentives for realising the benefits of DSD.

In setting out a generalized action plan with replicable drivers we appreciate the need to 'tailor-make' action strategies to suit the individual communication frames within different organisations and communities. That is why these drivers were crafted only following on from the experience of the use case previously mentioned. Further, we agree with the report on the need for external facilitation in promoting these drivers and fostering DSD. The Report indicates that certain organizational frameworks may already have in place such external supports around network-dependent sectors. Accepting this to be the case but not the norm, we have focused down on two external facilitators that seem important in all DSD contextual iterations. These are:

- *Data marked transition* – market forces and institutional facilities that are amenable to the premises of DSD and do not frustrate the empowerment of vulnerable data stakeholders through pre-existing power asymmetries. Open finance is a case in point.
- *State oversight* - as with the concept of enforced self-regulation, the state should act both as an intermediary to see that principles are complied with, and best practice confirmed. In addition to a monitoring role, state regulators can, if necessary, step in to shore up safe data spaces if the context requires external bolstering.

Understanding these qualifications and pre-conditions we move on to the identification of individual *drivers for action.* So that this plan will easily fit into a variety of safe space settings, and to maximise its uptake, the drivers selected are simple, minimal and dynamic. In settling on essential drivers, we have been mindful of the criticisms levelled at many principle-based regulatory approaches – that their language is too abstract, too open to interpretation and does not always speak across the ecosystem. In addition, the drivers will need to be sufficiently inter-operable so that they can complement any underlying principles, and evolving code of conduct. Finally, we appreciate it is presumptuous to impose drivers on organisations and communities that are yet to engage with DSD. With this in mind, the drivers are proposed to kick-start their application through *co-creation implementation exercises* with data stakeholders in different safe data space contexts.

Working with the assistance of regulatory and governance endeavours focused on safe (trustworthy) data spaces, the following action plan and its drivers are proposed with the intention taking the conditions for digital self-determination and enabling its activation as a vibrant and effective data access and management regime. Each driver should not be viewed as discrete and progressional, but rather working as an inter-operative scheme.

INCLUSION:

At the outset it is important to identify the stakeholders who have an interest in DSD in any particular safe digital space, the nature of the data over which they may have claims, the relationships between stakeholders and the duties/responsibilities to each other depending on the power they exert over data in that space. The identification process can be a communal exercise but is primarily the responsibility of stakeholders with most power over data in that space and who wish to use that data for any secondary purpose. Once identified it is necessary to maintain a register of inclusion to ensure that data-subject interests are adequately recognized and included in the DSD process. The register again should be maintained collectively and managed by the stakeholders with most power over data in that space.

EDUCATION:

Once stakeholders are identified and included, they need to be informed and educated about their data or data in which they have an interest which is held/used/intended to be used by other stakeholders in that space. The duty to inform and educate rests with stakeholders who hold/use/intend to use or reuse such data. A log should be kept by the stakeholders with this duty on how they have discharged their duty.

ENGAGEMENT:

DSD is a self-regulatory strategy that depends on the engagement of stakeholders in open communication and negotiation over data. If the engagement is either not positive or respectful, then the digital space is not safe. Engagement, therefore, is crucial to the achievement of respective data interests through data control and management. With the data subject's interests being paramount in DSD the pathways for engagement need to be open, informed and mindful of prevailing data power asymmetries. To promote positive and respectful engagement, the stakeholder 'community' within any DSD context should agree terms such as the preferred medium for communication, nominated contact persons, turn-around time for replies to correspondence and person-to-person communication.

MOTIVATION:

Digital spaces can be safe, inclusive and operate with respectful engagement, but this will not guarantee all stakeholder participation. Particularly for vulnerable data-subjects who have up until this point been disempowers, ignored or largely without trust in regulatory mechanisms, the motivation for participation may be challenging. It is important when parties are considering the benefits of participating in DSD, that potential stakeholders make clear to each other what they can offer as a consequence of participation. For instance, data storers/ providers can offer at minimum to data-subjects information about the personal data they share and how it has been/will be used. Data-subjects in turn, if they are willing to trust data storers/providers may be willing to authenticate their data and open-up further access to personal data for agreed uses. To determine mutual interests as motivations some participants in DSD contexts may settle some simple agreements between parties regarding duties, obligations and expectations from engagement that will also act to further sustain trusted relationships.

INTEGRITY:

DSD is a process that enables data integrity and the protection of the integrity of data subjects in the control and management of their data. This is a fundamental and prevailing pre-condition for DSD. A market consequence of data/data-subject integrity is the potential for subject validation of personal data and thereby an increase in the integrity of data down pathways of access. This consequence of the open storage, provision and use of data not only protects the interests of data subjects in their data, but will improve the efficacy of data as it is then accessed and negotiated in agreed data marketing. In this way data integrity and re-assurance becomes a motivation for participation in DSD.

ACCOUNTABILITY:

DSD is a dynamic process. It will succeed or fail on the establishing and maintenance of trusted relationships about data use. Transparency around the storage, provision and use of data is an important factor in establishing and maintaining trust. However, openness alone will not always ensure trust between stakeholders. In fact, openness about data use may initially damage trust until good data use practices are agreed. DSD is necessary because a lack of openness or problematic data storage, provision and use could endanger the possibility of trust when data is transacted. As has been revealed with social media platforms, even conditional consent requirements or privacy protocols will not always bring trust. Sometimes even ethical standards, and product safety/risk minimizing will not guarantee trust. Trust, once established, must be continually nurtured and confirmed. Recognising this it is essential accountability mechanism should be built into safe data spaces so that stakeholders with greatest power over data in particular, can regularly be required to confirm that they are complying with the spirit of DSD in their data management practices. This should be more than a tick-box audit. *Depending on the nature, extent and duration of any DSD context, stakeholders can agree to nominate a data steward/custodian who will be responsible to ensure that accountability mechanisms are operational and inclusive, providing satisfaction to all parties.*

SUSTAINMENT:

DSD should be habitual and not viewed as a process for curing already problematic data control inequalities. However, due to the current novelty of DSD and the possible resistance to open data relationships in the minds of some stakeholders, sustainability needs commitment. Communities and markets that practice DSD will develop trusted data relations whether these be commercial or social, that will perpetuate more sustainable market arrangements and social bonds where data is concerned. *To convince market players and community stakeholders who may have been at odds with each other over data management prior to DSD, that this new approach offers a genuine alternative to contestation, advocates of DSD will need to engage in community/market awareness programmers and consensus-building exercises, to spread the message of DSD to those who would benefit from its operation*.

CONFLICT RESOLUTION:

Implementing and embedding DSD will not be without its challenges. As with any data relationship there may be disagreements about who has what interests and whose interests should prevail in any management or control encounter. Indeed, data interests will evolve as data is used and therefore apportioning such interests and seeing principal stakeholders are empowered to enjoy the benefits of their data may necessitate negotiation. So that conflicts over data interests do not derail the respectful and trusted engagement at the heart of effective DSD, there may be occasions where conflicts require resolution.

In the maintenance of safe data spaces, the contextual identification conditions in that space that may lead to conflict should be constantly considered by stakeholders so that amelioration can be attempted before conflict emerges. *Such amelioration requires continual, informed and responsive conversations between stakeholders about their legitimate expectations over the course of DSD.*

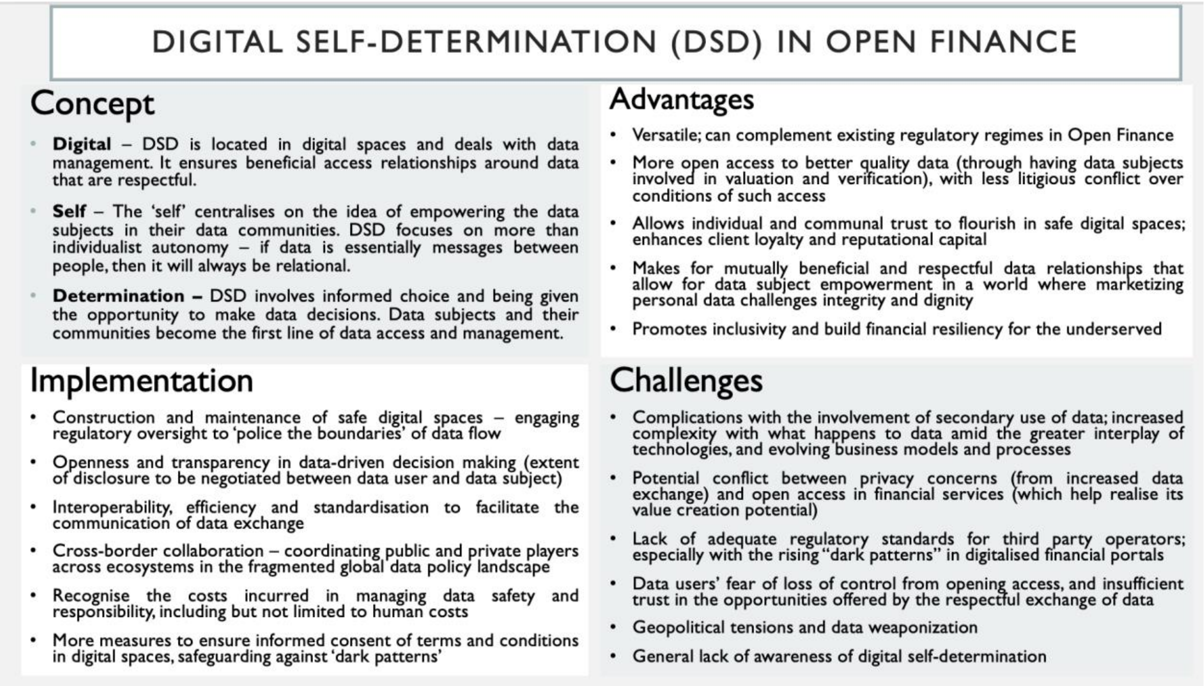
These conversations need to be informed by earlier conflict occasions and dynamics and their evolution. At this pre-emptive stage potential conflicts can be mediated, and conflict-generating conditions can be moderated, building true trust relationships. Data-subjects need to be provided with the information they believe may ameliorate power dependencies and social exclusion on which conflict feeds. Information sharing at this stage is imperative if fear and perceived risk of data abuse are to be addressed.

Most importantly, the 'learning from experience' dimension of conflict as a tool for social bonding as much as a force for disruption needs recognition. Once a conflict has been predicted and talked through, or identified and resolved via information sharing, interest compromise and mutual respect, the face of the DSD experience will become more trusting.

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Centre for
AI and Data Governance

Appendix: Outcomes for Use Case Studio



DIGITAL SELF-DETERMINATION (DSD) IN OPEN FINANCE

Concept

- **Digital** – DSD is located in digital spaces and deals with data management. It ensures beneficial access relationships around data that are respectful.
- **Self** – The 'self' centralises on the idea of empowering the data subjects in their data communities. DSD focuses on more than individualist autonomy – if data is essentially messages between people, then it will always be relational.
- **Determination –** DSD involves informed choice and being given the opportunity to make data decisions. Data subjects and their communities become the first line of data access and management.

Advantages

- Versatile; can complement existing regulatory regimes in Open Finance
- More open access to better quality data (through having data subjects involved in valuation and verification), with less litigious conflict over conditions of such access
- Allows individual and communal trust to flourish in safe digital spaces; enhances client loyalty and reputational capital
- Makes for mutually beneficial and respectful data relationships that allow for data subject empowerment in a world where marketizing personal data challenges integrity and dignity
- Promotes inclusivity and build financial resiliency for the underserved

Implementation

- Construction and maintenance of safe digital spaces – engaging regulatory oversight to 'police the boundaries' of data flow
- Openness and transparency in data-driven decision making (extent of disclosure to be negotiated between data user and data subject)
- Interoperability, efficiency and standardisation to facilitate the communication of data exchange
- Cross-border collaboration – coordinating public and private players across ecosystems in the fragmented global data policy landscape
- Recognise the costs incurred in managing data safety and responsibility, including but not limited to human costs
- More measures to ensure informed consent of terms and conditions in digital spaces, safeguarding against 'dark patterns'

Challenges

- Complications with the involvement of secondary use of data; increased complexity with what happens to data amid the greater interplay of technologies, and evolving business models and processes
- Potential conflict between privacy concerns (from increased data exchange) and open access in financial services (which help realise its value creation potential)
- Lack of adequate regulatory standards for third party operators; especially with the rising "dark patterns" in digitalised financial portals
- Data users' fear of loss of control from opening access, and insufficient trust in the opportunities offered by the respectful exchange of data
- Geopolitical tensions and data weaponization
- General lack of awareness of digital self-determination