SMU SINGAPORE MANAGEMENT UNIVERSITY | Centre for AI and Data Governance

12 FAQs on Digital Self-Determination

Mark Findlay
Professorial Research Fellow and Director
Centre for AI & Data Governance

25 February 2022

Digital Self-Determination (DSD) is a novel concept of constitutional self-regulation that approaches responsible data access away from rights, sovereignty and ownership. Instead, it centres on empowering data subjects in safe digital spaces. As the theoretical foundations of DSD begin to find grounding in contextual applications, it is important to clarify the key factors that differentiate DSD from traditional approaches to data access and management. As such, we introduce a bite-sized Q&A guide at 12 principle issues essential to understanding and defining DSD, along with some of the main challenges and opportunities it faces.

1. ‘What are three factors most crucial to defining Digital Self-Determination (DSD)?’
   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, to oversee their sense of self in the digital sphere. 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, management and use.

2. ‘Why is DSD important in the data ethics debate today?
   Data ethics is a principled approach to the application of data in the development of AI. Most ethics guideline frames are created by and directed towards those who employ data for commercial purposes, and the data subject is a passive recipient of ethical decision-making or otherwise. DSD requires safe data spaces in which respectful relationships can be developed around data subjects and their communities. Ethical data use, concerned to enhance safety and respect is an important agent in ensuring the pre-conditions for DSD.

3. ‘What would encourage stakeholder participation in DSD when previously they have thought in terms of data and legal rights?’
   Very simply, more open access to more data with less contestation over the conditions for such access. Currently struggles over data as property, and data sovereignty do not offer congenial resolutions of mutual interests and benefits in data. With the exponential pressure, social and economic, to share data, many current commercial reuse practices are clandestine and potentially exploitative. Unless more mutual and respectful access pathways such as DSD can

be enabled, external regulation over data protection will proliferate and contestation will become the default.

4. ‘How can DSD operate in a communal relationship of trust/duty/respect?’
Data is neither entirely personal nor entirely commercial/business. It involves the data subject, the data she generates and how this data flows and circulates within data communities. When the digital spaces for such circulation are safe, data relationships can develop respectfully. Trust between data subjects and data recipients will emerge in safe digital spaces, there being a duty on both data subjects and data users to respect data flows and the legitimate mutual interests of participants in data exchanges.

5. ‘What issues such as commercial arrangements, information deficit, contested interests make the management of data by the data subject a complicated matter?’
The negative consequences for data subjects in much current data marketizing is that they are not informed that their data is being used and commodified, and as such have no say in whether and how this should happen. Data subjects can’t even withhold data if they are unaware of what happens to their messages once they are released. Power imbalances in many data markets leave data subjects open to exploitation. Many personal data protection regimes require data subject activation and therefore cannot remedy such situations. Contrarily, DSD recognises that including data subjects at the outset will not deny data marketing. Rather, it will create responsible expectations governing market relationships and open up possibilities for greater informed access.

6. ‘What makes a digital space ‘safe’ in the context of DSD?’
Safety is a matter for data subjects (and their communities) to experience and should be a condition of data access for responsible data users. Openness is the first requirement for safety to flourish. Next, respectful engagement between data communicators is essential. A duty to maintain safety rests on all who engage data within these spaces. External agencies may have a role in ‘policing the boundaries’ of safe data spaces and the transit between actual and virtual data flows.

7. ‘What is DSD beyond data portability and data access?’
Data portability empowers the data subject to have a say or some control in the storage and flow of her data. DSD offers a similar facility, but is more interactive between data subjects and data users. DSD may progress no further than informing data subjects of their data’s whereabouts. But more than this, DSD enables data subjects to have choices in much more than mobility, including how their data is managed in a variety of safe digital spaces in which it resides.

8. ‘Where is the place for regulators in the context of DSD and what are some of the current regulatory hurdles that DSD faces, if any?
Any regulatory regime that works out of a ‘data property/data rights’ frame will require modification to be compatible with DSD. DSD can run in parallel with such regulatory regimes, but the potential for ‘regulation shopping’ will add confusion. Personal data protection regimes can be modified to accommodate DSD, but will be required to protect the safety of digital spaces and duties for respectful engagement, rather than restrict access based on claimant rights.

DSD is an internal, consensual form of constitutional self-regulation. As such, it is distinct from more command-and-control regulatory approaches.

9. ‘Is there stakeholder resistance to DSD? How can DSD overcome those challenges?’
There could well be resistance, particularly from stakeholders who are marketizing data in ways that are not respectful of data subject interests, or responsible in terms of access fairness. But resistance may be based on an assumed loss of market benefit by more open and inclusive access practices. Instead, DSD offers healthy and sustainable data market conditions, where responsible access means more open, trusted and respectful data pathways which should minimise log-jams and contestation when access is suspected and revealed. DSD, if supported, will offer an alternative regulatory option to external command and control intervention.

10. ‘How could the costs incurred by ensuring data safety and responsibility in DSD be accounted for?’
Whatever costs accrue from DSD compliance will be more than outweighed by the freeing up of responsible access. It is similar to the reservations expressed when compulsory licencing entered the market as a buffer to patent exclusivity. What happened in this case was market invigoration and diversification, which overcame any initial loss of rights returns.

11. ‘How would DSD change the global and local outlooks for data access and usage?’
Since it does not talk the language of property and sovereignty, DSD should not be spatially or temporally bound. DSD works in safe digital spaces, and these can exist in any virtual or actual environment. As such, law’s engagement with DSD is much more likely to be at the level of shared norms and values, rather than delimiting jurisdictionally bound trade routes. With the recognition that data is impossible to secure in spatial and temporal confines, and that open access is more likely to stimulate innovation than rights exclusion, DSD is a contemporary agenda for the globalisation of data.

12. ‘How can DSD emerge against weaponization of data and national data interests?’
States claim data sovereignty for two primary motivations. The first is national security and aligned with that is economic advantage. It will become more and more apparent that national security and economic advantage are more endangered through irresponsible data access (such as hacking through to unregulated trade) than by opening up personal data to the understanding and management of data subjects. Pragmatically, nation states can have little effect over data sovereignty when at the same time they seek the benefit of open access. In addition, one of the greatest guarantees of data integrity and responsible data use is data subject empowerment.