The Cube of Sharing

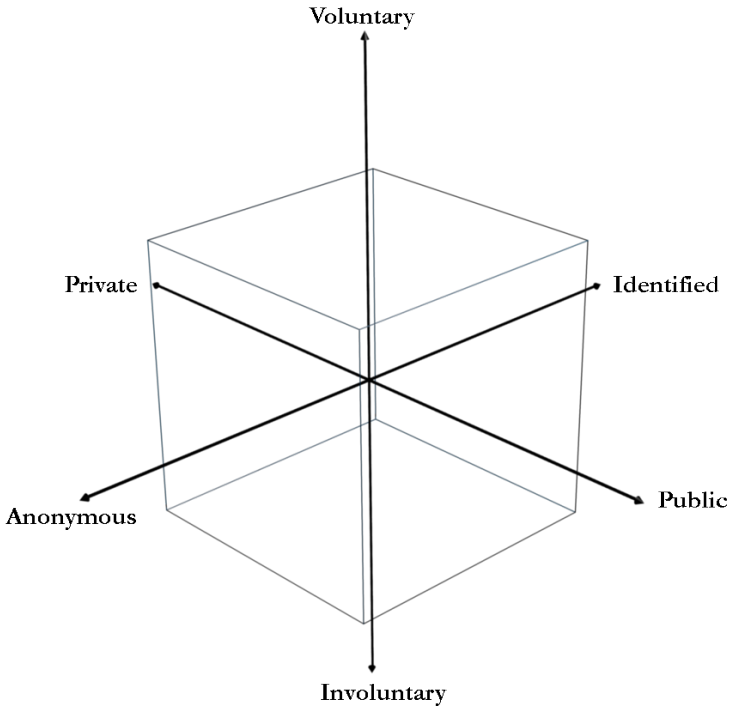
Clément Vidal

Vidal, C. 2014, *The Cube of Sharing*, published in French as « Le cube du partage » in *La Revue du Cube*, **6**, pp 65-68.
English: https://doi.org/10.5281/zenodo.1401733
French: http://lecube.com/assets/revue/006_revue-lecube_partager.pdf

In the material world, sharing means dividing resources. If I share a cake with you, I can have only half of it. In the informational world, sharing means multiplying. If I share a digital photo with you, we both have it in our computers. Economists call material resources "rival", and resources which do not obey conservation laws, "non-rival".

This does not make the world of information magical, as it is not free of material constraints. The capacities for information processing, network bandwidth and memory capacity all directly depend on physical hardware. But for most purposes, the material and energetic constraints become negligeable. Processing, sending and storing thousands of emails consumes a tiny amount of energy, processing power, bandwidth and memory. The main point is that in our information society, sharing doesn't mean divising anymore, it means multiplying.

Yet, a multiplication process quickly grows exponentially. Are we always in control about the information we share? How much do we want to share? What if private information is collected, stored, processed and shared without our consent? Are we always ready to share information on behalf of our official identity? What are the best information sharing policies which could benefit both individuals and society? To explore these questions, I propose the following "cube of information sharing":



It represents three axes:

1) Private and public sharing

2) Voluntary and involuntary sharing

3) Anonymous and identified sharing

Note that the axes are more of a continuous rather than discrete nature. Let us discuss those dimensions and their interactions.

The first axis distinguishes between private and public sharing. In general, if I write an email to one person, it is destinated to that person only, and not to the whole world. An interesting question for the future is whether we are going to share more easily with other humans or with machines. By machine, I mean here a sofware agent, such as algorithms in Google's mail service which read the content of emails in order to offer customized advertisement. If this procedure is fairly secure, I could trust it much more than humans doing the same job. Indeed, we could not tolerate the idea that Google employees could compile the most ridiculous or pittiful emails to read them aloud and have a good laugh during their coffee break. The key concept here is trust. Ideally, open source and strong cryptography are basic ingredients to build trust in the infosphere. Once this will be established, we will be more likely to trust reliable algorithms and machines than humans who are prone to emotional reactions and failures.

The second axis plays with the limit of the concept of sharing. Involuntary sharing is not sharing anymore. In principle, we want to share only information that we are willing to share, and not more. Unfortunately, we are often out of control of what we share. On social networks, people can easily re-share and propagate a message or photo which was not originally meant to be diffused. We certainly do not know all the friends of our friends. We also know that governemental agencies, and the NSA in particular, can snoop into the private life of nearly all internet users. However, note that they keep these data private. A bit like a paparazzi having thousands of photos and documents about your whole life, they can decide to release them, whenever, if ever, they strategically want.

The third axis is quite important because it shows that we can be willing to share more or less depending on whether we are identified as anonymous, with a pseudonym or with our real identity. Imagine that you are a fan of philately, but you know that your boss finds it ridiculous. You still want to connect with online communities of philatelists. There is really no need to risk to compromise your relationship with your boss and to use your real name. But you don't want to be anonymous either within your philatelist community, as you know that you will further interact with them. In this case, the right choice is to take a pseudonym, so you can have the benefit of the private community without endangering your public image.

The big data which stems from the information we all create and share, willingly or not, can be very useful at a societal level. However, in most cases it remains very useful even if it is anonymized. Let me give you an example. I can be willing to share with the public transports company my weekly transport habits, as it can help them to build better network infrastructures to serve me and other users.

However, there is absolutely no need to associate my identity with this data. The improvement of traffic fluxes doesn't need to know who is who.

Furthermore, I would like to propose that even if by default the data of where we go is used by transport engineers, for whatever reason, we should still be able to refuse this data collection and usage. But this choice, which would not be beneficial at the level of society could become a paid-choice, which is the prize to pay for this non-cooperation. The same holds with web-based email clients, which display advertisments depending on the content of emails. If I can trust software agents to read my mail for the purpose of targeted advertisment and benefiting from a free email service, fine. But I should have the option to pay to have full privacy and no advertisment.

We are still making mistakes in how we share information, at personal and national levels. The NSA, thinking they had build an enormous strategic advantage have lost and are losing a lot, something which can not be bought easily, and which is hard to restore: trust. For the USA, the Snowden revelations about massive surveillance have created a huge breach in trust both for international relations, and for their most successful businesses: Microsoft, Apple, Facebook or Google. This remains valid even if these companies were not aware of this massive surveillance. It is part of their mission to secure the privacy of data of their customers.

The freedom of expression, innovation and creativity require that we have options and secure choices to share information with whom we want and on behalf of either our real identity, a pseudonym, or anonymously. It is more than time to face and take up these challenges.

Further reading:

Brin, David. 1999. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. Basic Books.

Helbing, Dirk, and Stefano Balietti. 2011. "Big Data, Privacy, and Trusted Web: What Needs to Be Done". SSRN Scholarly Paper ID 2322082. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2322082.