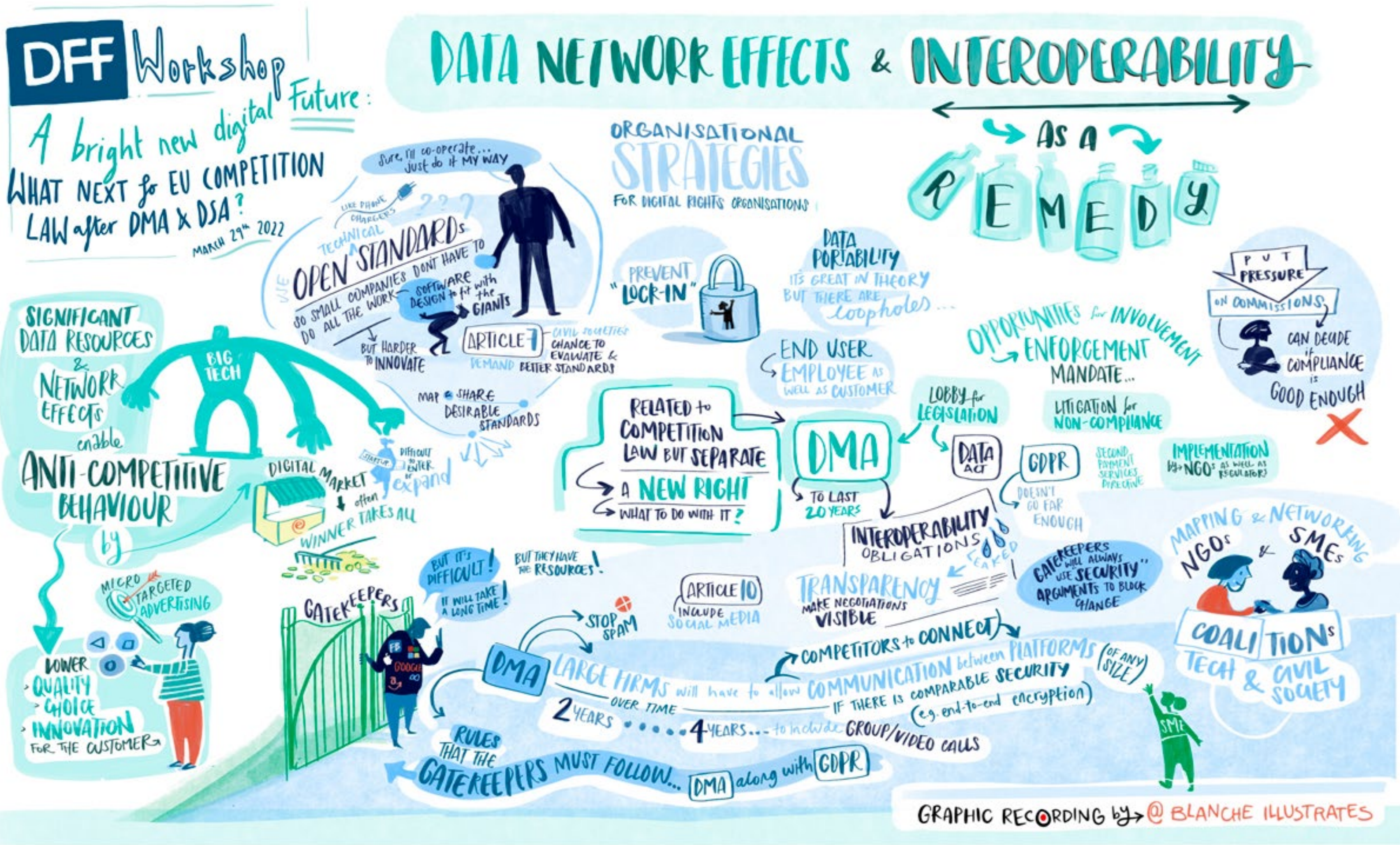
Data, network effects and interoperability

Facilitated by Ian Brown



DFF Workshop
A bright new digital Future:
WHAT NEXT for EU COMPETITION LAW after DMA & DSA?
MARCH 29th 2022
DATA NETWORK EFFECTS & INTEROPERABILITY
AS A REMEDY
ORGANISATIONAL STRATEGIES FOR DIGITAL RIGHTS ORGANISATIONS
Sure, I'll co-operate... Just do it MY WAY
LIKE PHONE CHARGERS
???
USE TECHNICAL OPEN STANDARDS
SO SMALL COMPANIES DON'T HAVE TO DO ALL THE WORK
SOFTWARE DESIGN to fit with the GIANTS
BUT HARDER TO INNOVATE
ARTICLE 7
CIVIL SOCIETIES CHANCE TO EVALUATE & DEMAND BETTER STANDARDS
MAP & SHARE DESIRABLE STANDARDS
PREVENT "LOCK-IN"
DATA PORTABILITY
IT'S GREAT IN THEORY BUT THERE ARE loopholes...
END USER
EMPLOYEE AS WELL AS CUSTOMER
OPPORTUNITIES for INVOLVEMENT
ENFORCEMENT MANDATE...
PUT PRESSURE ON COMMISSIONS
CAN DECIDE if COMPLIANCE is GOOD ENOUGH
SIGNIFICANT DATA RESOURCES & NETWORK EFFECTS enable ANTI-COMPETITIVE BEHAVIOUR by
BIG TECH
STARTUP
DIFFICULT to ENTER or expand
DIGITAL MARKET
often WINNER TAKES ALL
MICRO TARGETED ADVERTISING
LOWER
QUALITY
CHOICE
INNOVATION
FOR THE CUSTOMER
RELATED to COMPETITION LAW BUT SEPARATE
A NEW RIGHT
WHAT TO DO WITH IT?
DMA
TO LAST 20 YEARS
LOBBY for LEGISLATION
DATA ACT
GDPR
DOESN'T GO FAR ENOUGH
SECOND PAYMENT SERVICES DIRECTIVE
LITIGATION for NON-COMPLIANCE
IMPLEMENTATION by NGOs AS WELL AS REGULATORS
INTEROPERABILITY OBLIGATIONS
LEAKED
TRANSPARENCY
MAKE NEGOTIATIONS VISIBLE
GATEKEEPERS WILL ALWAYS USE "SECURITY" ARGUMENTS TO BLOCK CHANGE
MAPPING & NETWORKING
NGOs & SMEs
COALITIONs
TECH & CIVIL SOCIETY
SME
BUT IT'S DIFFICULT!
IT WILL TAKE A LONG TIME!
BUT THEY HAVE THE RESOURCES!
GATEKEEPERS
FB
GOOGLE
ARTICLE 10
INCLUDE SOCIAL MEDIA
STOP SPAM
DMA
LARGE FIRMS will have to allow COMMUNICATION between PLATFORMS (OF ANY SIZE)
COMPETITORS to CONNECT
IF THERE IS COMPARABLE SECURITY (e.g. end-to-end encryption)
OVER TIME
2 YEARS ..... 4 YEARS... to include GROUP/VIDEO CALLS
RULES THAT THE GATEKEEPERS MUST FOLLOW... DMA along with GDPR
GRAPHIC RECORDING by @ BLANCHE ILLUSTRATES

DFF Digital Freedom Fund

01. What was this session about?

1. Participants discussed the impact of key data resources and network effects in the digital environment and how far they enable anti-competitive behaviour by platforms and other Big Tech companies:

> A firm with a large amount of data about its customers often has a significant advantage over potential competitors in providing services (such as product recommendations), discouraging customers from switching to competitors, improving its services (e.g. through machine learning model training), and developing new related services.

> A firm with many users can be more attractive to existing and new users (e.g., a messaging or social networking service) and to other types of customers (e.g., advertisers; drivers; restaurants) — so called direct and indirect network effects.

02. Why should digital rights organisations care?

1. Due to these and other factors, digital markets are often “winner takes all”, with one firm taking a very large market share (e.g. search and social media in most EU member states) and competitors finding it very difficult to enter or expand into the market. This means customers are likely to face higher prices and/or, in the case of advertising-supported “free” services, lower quality, choice and innovation, including greater intrusion to enable micro-targeted advertising.

2. At the same time, interoperability requirements could lead to new risks. For example, left unchecked gatekeepers could develop proprietary interoperability standards, which could hinder interoperability in practice.

03. Is an interoperability mandate the answer and how do we enforce it?

1. Requiring dominant or gatekeeper firms to enable other companies to connect to their services can be a powerful remedy for anticompetitive data and network effects, in various forms below. Each of the relevant statutes has specific enforcement opportunities. (More detail is overleaf.)

04. Four related remedies

1. **Data portability** (GDPR Art.20) — individuals have right to move their personal data from one service to another, directly if possible, reducing switching costs. Vague, underenforced.

2. **Real-time data portability or data interoperability** (Payment Services Directive 2 and Digital Markets Act Art.6(1)(h)) — user can authorise one service to access their data in another (e.g. financial planning tools using live bank account data; farmer gets advice on reducing pesticide use based on data from their tractor sensors; consumer gets advice on energy or telecoms services based on usage).

3. **Functional interoperability** (DMA Art.6(1)(f); competition law) — user of one service can, with permission, cause another to take an action (e.g. make a payment; send/receive messages; interact with users of another social network; use different client software to access a service; control IoT devices; charge electric cars using all chargers).

4. **Data sharing** (DMA Art.6(1)(j); Data Act; competition law) — firms required to share key data resources with competitors/customers/governments.

05. Ways for digital rights organisations to get active

1. **Enforcement of user remedies:** Digital rights organisations could engage with consumers and SMEs in the use of these remedies.

2. **Support of regulatory action:** In addition, Art. 7 DMA makes the interoperability mandate subject to further specification by the Commission: it could, for example, decide that a gatekeeper's interoperability actions do not meet its legal requirements and require, among other things, better documentation, the creation of a stakeholder forum, etc. Digital rights organisations could put pressure on Commission to make use of those powers.

3. **Standard setting**: Digital rights organisations could work together to map developing official and commercial interoperability standards and work with smaller companies to develop baseline standards that are designed to protect the digital rights of consumers. Specifically, digital rights organisations could help tech companies understand civil society concerns that go beyond the commercial and information security concerns that those tech companies are likely to focus on.

Sources of market power for large firms/platforms	Interoperability or related remedies	Specific issues (*=minor, **=major)
Access to individual customer data to provide customised services and adjacent services	Real-time data portability/data interoperability (under individual customer control) Requirement to support user data stores (Much) stricter enforcement of data minimisation and purpose limitation elements of data protection law	Customer needs accounts with all services s/he wishes to interact with, and faces take-it-or-leave-it contract terms requiring eg consent for profiling (which can also be addressed with consumer protection measures) ** Incentive to greatly increase profiling of users (needing greater enforcement of data minimisation/ purpose limitation in data protection law)*
Access to large-scale raw customer data for analytics/ product improvement	Mandated competitor access to statistical (eg search query and clickstream data) or raw data (likely in pseudonymised form)	Significant data protection issues (difficulty of anonymisation) with raw data ** Reduced incentives for data collection *
Access to large-scale aggregate/ statistical customer data for machine learning etc.	Mandated competitor access to models, or specific functionality of them via APIs (eg checking content against hate speech models)	Potential data protection issues (since firms would be given access to competitors' customer records without those individuals' consent) (need to consider mitigations such as differential privacy) * Reduced incentives for data collection and model training **
Ability to restrict competitor interaction with customers (eg send/receive messages, share content, collaborative editing, make payments, allocate jobs)	Requirement to support open/ publicly accessible APIs or standardised communications protocols (such as from the ITU, IETF or W3C)	Complexity of designing APIs/ standards, while preventing anti-competitive exclusion *
Availability and use of own core platform services (eg monetisation and identity) to increase "stickiness"	Govt coordination and funding for development of open infrastructural standards and components Requirement for platforms to support/integrate these standard components	Technical complexity of full integration of standard/ competitor components into services/design of APIs to enable this, while preventing anticompetitive exclusion ** Potential pressure to incorporate government surveillance functionality in standards

About the Digital Freedom Fund

The Digital Freedom Fund supports strategic litigation to advance digital rights in Europe. With a view to enabling people to exercise their human rights in digital and networked spaces, DFF provides financial support for strategic cases, seeks to catalyse collaboration between digital rights activists, and supports capacity building of digital rights litigators. DFF also helps connect litigators with pro bono support for their litigation projects. To read more about DFF's work, visit: **www.digitalfreedomfund.org.**

DFF Digital Freedom Fund