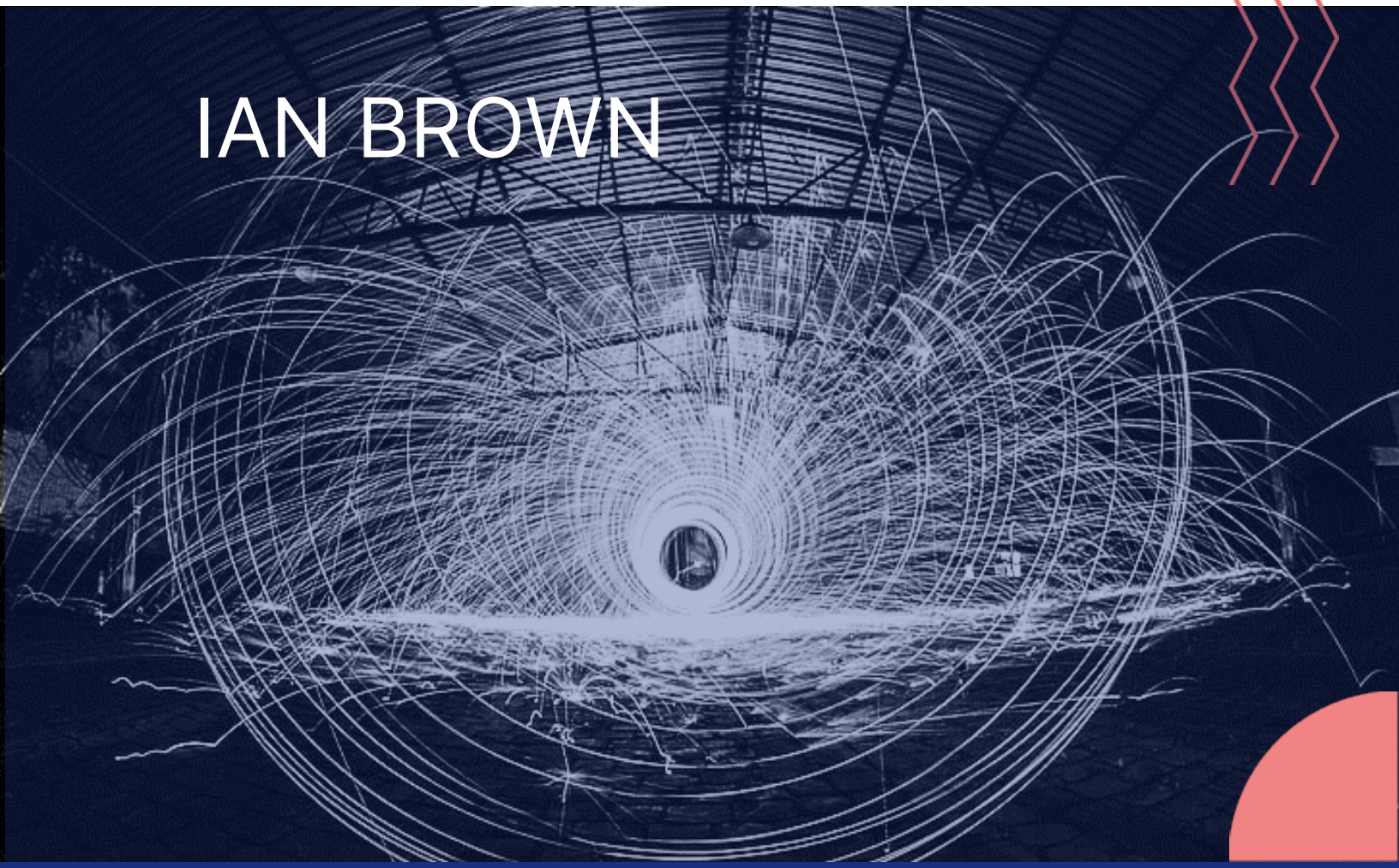
NOV 2020

THE TECHNICAL COMPONENTS OF INTEROPERABILITY AS A TOOL FOR COMPETITION REGULATION

IAN BROWN



ofa OpenForum Academy

This report covers the main technical and related elements supporting the creation of interoperable systems: open APIs and protocols; the standardisation process; data access and sharing; device neutrality; and open identities. It considers the type, extent and scope of interoperability obligations that could be imposed on large online platforms, and the practical consequences for them. And it develops a new scale of interoperability obligations, where regulatory action to require a platform to move up the scale gives users more freedom in terms of the services and software they can use to interact with those platforms and their users, but may require increasing levels of regulatory action/market intervention and technical complexity. The levels are as follows, starting from the *status quo* at level 0:

1. *Platform-permissioned vertical interoperability*: users can connect their own account on complementary services from a third party to a platform, with its express permission. Users can use major platform IDs to log in to other services. Regulators may impose transparency, feedback and stability requirements, and limit self-preferencing.
2. *Open vertical interoperability*: users can connect their own accounts and open IDs on complementary services, or apps, from a third party, to a platform, without the platform's permission. This would enable *real-time data portability*.
3. *Public horizontal interaction* (no external user authorisation needed), for publication and messaging with competing services.
4. *Private horizontal interaction* (external user authorisation needed at this and higher levels):
    a) *Sharing* – Platform users can share resources (such as a feed) with a limited number of readers (who should not need an account on that platform).
    b) *Messaging* – an account owner can authorise any other user to send them (or groups they administer) messages or other types of content.
    c) *Social graph*: a platform user can authorise a third-party service to access enough details of their contact list to identify contacts present on both.
5. *Seamless horizontal interoperability*: users have the ability to use directly competing services to a platform's own for:
    a) *Componentisation* – to replace components on a platform.
    b) *Seamless interaction* with its users.

Intended audience: this paper is intended to support civil society and parliamentary groups developing positions on *ex ante* competition rules in the EU's proposed Digital Markets Act, and digital competition reforms in other jurisdictions.

Acknowledgements: The author thanks all the interviewees for contributing their time and expertise, as well as Vittorio Bertola, Jon Crowcroft, Gerben and Hamed Haddadi for their advice.

Funding: This research was supported by the Open Society Foundations Information Programme. All unattributed analysis and opinions expressed are entirely the author's own.

About the author

Dr Ian Brown is visiting CyberBRICS professor at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro. He was previously Principal Scientific Officer at the UK government's Department for Digital, Culture, Media and Sport; Professor of Information Security and Privacy at the University of Oxford's Internet Institute; and a Knowledge Exchange Fellow with the Commonwealth Secretariat and UK National Crime Agency. His books include Cybersecurity for Elections, Regulating Code, and Research Handbook on Governance of the Internet.

Contents

Figures

Introduction

Interoperability is a technical mechanism for computing systems to work together – even if they are from competing firms. An interoperability requirement for large online platforms[1] has been suggested by the European Commission as one *ex ante* (up-front rule) mechanism in its proposed EU Digital Markets Act (DMA), as a way to encourage competition.[2] The policy goal is to increase choice and quality for users, and the ability of competitors to succeed with better services. The application would be to large online platforms such as social media (e.g. Facebook), search engines (e.g. Google), e-commerce marketplaces (e.g. Amazon), smartphone operating systems (e.g. Android/iOS), and their ancillary services, such as payment and app stores.

The policy background to this ongoing legislative debate is covered in detail in Interoperability as a tool for competition regulation. This second report looks at the technical building blocks that should be considered in introducing such a requirement for large platforms.

As well as a review of relevant technical and computer science literature, this paper draws on 10 semi-structured interviews with software developers, platform operators, technical standards experts, current and former government officials, and academic and civil society experts working in this field.

[1] The Digital Services Act consultation defines this as "online platforms reaching a certain level of users and covering different types of services that are considered to have a particularly important impact and play a distinctive role as 'gatekeepers' to the services they provide. Since the present consultation itself inquires about the distinctive features, the impact and the potential measures, which need to be taken in relation to such platforms, this definition should be understood more as a description of possible features that identify large online platforms."
[2] European Commission DG Connect, The Digital Services Act package, 2 June 2020.

What are the building blocks of interoperability?

The most fundamental technical elements of interoperability are the open protocols and Application Programming Interfaces (APIs) that let interoperable systems communicate, along with standards for the data exchanges they facilitate. The EU has a well-developed process for initiating, supporting, and recognising technical standards that could be important in the evolution of detailed technical rules for interoperability.

Beyond that, regulators should consider issues of data portability and access (including Personal Information Management Systems), which were highlighted in all of the major recent digital competitions review. Device neutrality, provided for in a French Senate bill, would stop firms using control of devices such as PCs and smartphones to privilege their own services. Open identities, including the EU's eIDAS standards, can simplify the process of users accessing new services – reducing one important barrier to entry, while giving users the choice about whether such ID providers can profile their use of those services.

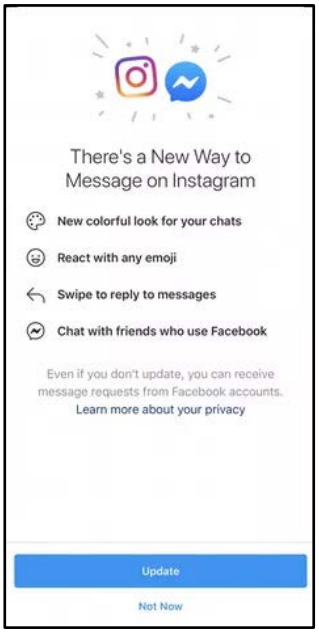


Figure 1 Facebook adds interoperability to Instagram chat

Open protocols and APIs

Interoperability between systems and software is achieved technically using Application Programming Interfaces (APIs) and communications protocols. An API is, according to the European Commission's Digital Services Act consultation, "a computing interface allowing access to a software or technical system and defining the conditions under which the system can be used. APIs typically intermediate in a standardised manner a series of data (and information) flows between computing systems."[3] A communication protocol similarly defines a set of messages that can be sent between two or more systems to share information and invoke features – via the Internet or other networks (or even on the same computing system).

Technical interoperability requires both syntactic (systems have a "language" to speak to each other, to request information and action) and semantic (the meaning of the information exchanged is understood by both parties) interoperability[4]

[3] *Ibid*.
[4] W Kerber and H Schweitzer (2017) Interoperability in the digital economy, JIPITEC Vol. 8, pp.39–58.

(although an interviewee added: "Syntax and semantics are like magnetic poles: it's hard to encounter one without the other.")

Two standards body expert interviewees classified interoperability layers similarly:

1. Syntactic interoperability, encoding content (RDF+XML, JSON-LD, etc.)
2. Semantic interoperability:
    a) RDF semantics: How to interpret a JSON/XML document as a graph.
    b) Semantics of the graph data: what does each node or edge mean (defined in ontologies/vocabulary).
3. Procedural interoperability (API, bureaucracy, race conditions etc.)

A startup developer interviewee noted the third level should include contracts and contractual provisions: "When data circulates, what protects people is consent, what protects organisations is contract. We want to standardise contracts also. Maybe not yet up to a point to have smart contracts, but at least a framework for legal personal data circulation. Many projects understand the legal issues we have already, but they work too much apart from each other. When you have telecom engineers like me, of course they want standards, they are our mindset, but for lawyers it's not the same. So, we have a lot of work to do to make them understand we need this legal infrastructure behind data circulation. It's a governance issue putting everyone around the table to discuss common infrastructure, common standards, and this is a governance issue."

Data formats (such as HTML) have been widely standardised in the last three decades (e.g. video standard MPEG, videoconferencing standard H.264, and the *de facto* then international standard office suite document standard from Microsoft) – the latter encouraged via public procurement rules and legal permission for reverse engineering (for example, Apple first made its iWork apps compatible with Office, and now there are many other compatible products, such as LibreOffice and Google Docs/Sheets/Slides).[5]

The mere existence of standardised data formats, however, is decreasingly useful for encouraging competition, as more and more user data are stored inside platforms' own systems, with limited access for competitors. Doctorow noted that in the mid-2000s, "despite a standard format for financial data interchange called OFX (Open Financial Exchange), few financial institutions were offering any way for their customers to extract their own financial data. The banks believed that locking in their users' data could work to their benefit, as the value of having all your financial info in one place meant that once a bank locked in a customer for savings and checking, it could sell them credit cards and brokerage services." It took a startup company (Mint) to create "screen-scraping" software to allow

[5] C Doctorow, Adversarial Interoperability: Reviving an Elegant Weapon From a More Civilized Age to Slay Today's Monopolies, EFF Deeplinks, 7 June 2019.

customers to access and download their own account data without cooperation from their banks. This was the precursor of the increasingly popular Open Banking national programmes in Europe and elsewhere.[6]

APIs can be invoked by one piece of software interacting with another on the same computing device (e.g. an application opening a file or asking a user a question via the underlying operating system, such as iOS, Linux or Windows), or running on two or more connected devices. Software running on different devices can similarly communicate using a protocol (or sequence of messages) over the Internet or other networks – for example, a mail app on a PC or smartphone downloading new messages (using an Internet Engineering Task Force (IETF) standard such as IMAP, or a company-specific API such as for Google's Gmail); or a Covid-19 contact tracing app exchanging random identifier numbers with nearby smartphones over Bluetooth Low Energy (using a protocol such as France's ROBERT, or Apple and Google's *de facto* Exposure API standard).

APIs and protocols can use *de facto* standards, set by their main developer, with more or less transparency and stability (or alternatively competitors discovering for themselves the details of interfaces using reverse engineering), and sometimes informal cooperation with other later users of those APIs/protocols; or formal standards, set by standards bodies such as the European Telecommunications Standards Institute (ETSI, responsible for the GSM and 3G mobile standards), the IETF (which sets Internet standards, such as for email), and World Wide Web Consortium (W3C, which sets standards for HTML and other Web protocols, and already created the social web standards ActivityPub and ActivityStreams, used by the interoperable Twitter-like service, Mastodon.)

Williams et al. suggest the requirement by regulators of the use of standard protocols rather than APIs is more appropriate for well-established, dominant platforms,[7] as shown in Figure 2:

[6] C Doctorow, Mint: Late-Stage Adversarial Interoperability Demonstrates What We Had (And What We Lost), EFF Deeplinks, 5 December 2019.
[7] H Williams, F Li and J Whalley (2006) Interoperability and Electronic Commerce: A New Policy Framework for Evaluating Strategic Options, Journal of Computer-Mediated Communication, Vol. 5, Issue 3.

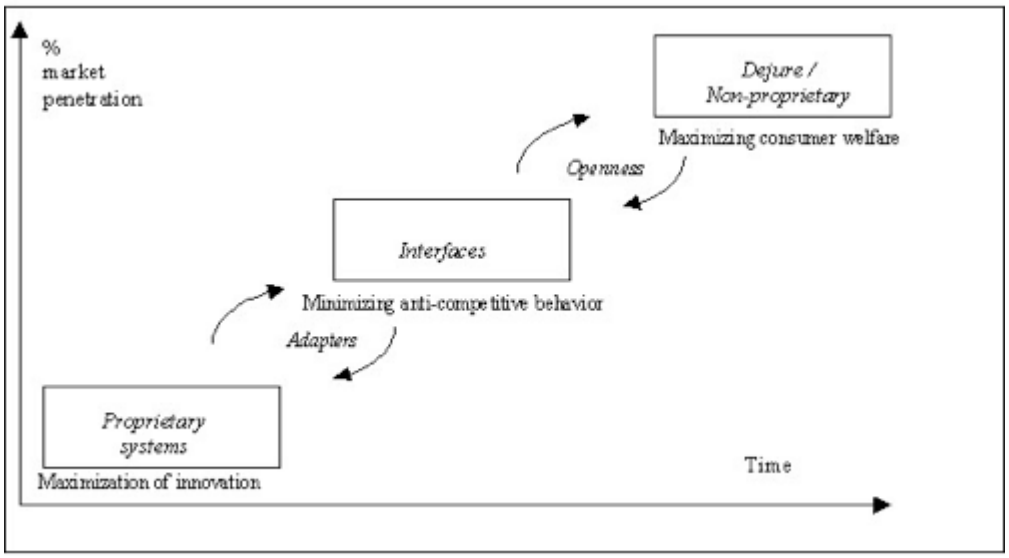


Figure 2 Williams et al. (2006), A framework for policy intervention

The Facebook investor presentation slide in Figure 3, published by the US House of Representatives' antitrust subcommittee, speaks for itself:

Facebook Investor Presentation[771]

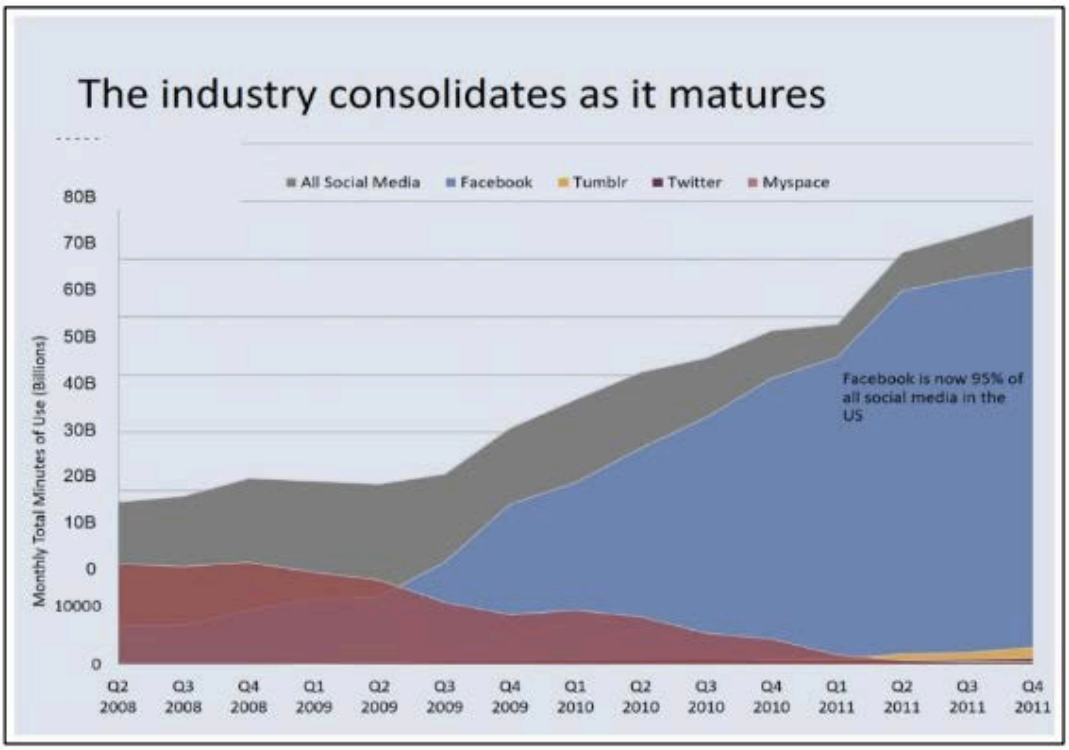


Figure 3 Facebook on social media consolidation

An SME engineer interviewee commented: "there is a fundamental philosophical difference between APIs and protocols that makes the latter much preferable: APIs represent an endpoint interface and are usually designed unilaterally by the party that provides them as a service to others, while protocols describe peer-to-peer communications and require the agreement of both peers." The French Conseil national du numérique also concluded: "the setting up a common protocol for one or more functionalities is preferred to opening existing APIs for large platforms."[8]

A frequent complaint from competitors is that a dominant platform "ecosystem" (collection of services) allows its own services privileged access to data and functionality. Competition Commissioner Margrethe Vestager's special advisers commented:[9]

[8] Google translation of Conseil national du numérique, Étude de cas sur l'interopérabilité des réseaux sociaux, 1 July 2020.
[9] J Crémer, A de Montjoye and H Schweitzer, Competition policy for the digital era (Luxembourg: Publications Office of the European Union, 2019), p.34.

> *If [ecosystem] privileged access to a user's data or connectivity with other services or Internet of Things devices allows a service from the ecosystem to offer a much better product, competitors will not be able to compete on the merit, e.g. based on the best algorithm. The multi-purpose use of data only makes this issue more prominent. Furthermore, the existence of some privileged APIs (with the consent of the user) might not be sufficient for a competitor to compete: 1) if the API made available to competitors is more limited (e.g. in functionalities, data it can access) compared to the API made available to the service that belongs to the ecosystem, or 2) the competitor cannot rely on the API to continue to exist and be available in the future. There indeed exist numerous examples of platforms discontinuing APIs as they grow larger or become dominant.*

London's Office of Technology and Innovation has drafted the following suggested contractual terms for London councils (local government authorities) to include when procuring systems, which ensure ongoing access for the council via open APIs, and hence the ability to avoid suppliers "locking-in" councils to future contracts:[10]

> *Wherever permitted according to the General Data Protection Regulation, all other relevant data protection legislation, and where they have control and rightful permission to use the data:*
>
> - *The system must have web APIs that enable the Council to give other applications full ability to send data to, or request data from it.*
>
> *Specific requirements for these APIs include:*
>
> - *All significant business functions should be available via API*
> - *APIs should enable live data to be queried in real-time*
> - *APIs should support "Time Based Extracts" (e.g. data changed after date "X") for both full system extracts as well as for more specific web API calls.*
> - *Any data that can be submitted by a user operating the system should also be able to be entered via API.*
> - *A complete register of all APIs must be provided to the council. All Open APIs must be discoverable.*

[10] London Office of Technology and Innovation, Tender Requirement for Data Access and APIs, working draft accessed 20 August 2020.

- *All APIs must come with comprehensive documentation.*
- *Where API access is restricted, a test API must be available. Ideally, test environment(s) should be provided that let developers test the API without affecting production environments.*
- *These features must be provided without additional charge or limitation that would prevent the Council from accessing, sharing and using the data through the API.*

A standards body expert interviewee noted: "Distributed systems are more burdensome than centralised systems. So, the legal environment must set positive incentives for decentralised systems, because otherwise the centralised will always prevail, as the Internet has shown the winner will take all. There we need to do research and talk to the engineers."

The EU legal framework for technical standards

Technical standards are an essential tool for reducing non-tariff barriers to trade within the EU's Single Market. In many EU Directives and Regulations, the European Commission and national authorities are given the power to encourage and even require the use of specific standards, and to support the creation of new standards when needed. As the European Commission put it in 2016:

> *Common standards ensure the interoperability of digital technologies and are the foundation of an effective Digital Single Market. They guarantee that technologies work smoothly and reliably together, provide economies of scale, foster research and innovation and keep markets open. Effective interoperability guarantees that connected devices such as cars, phones, appliances and industrial equipment can communicate seamlessly with each other, regardless of manufacturer, operating system, or other technical components. Open standards ensure such interoperability, and foster innovation and low market entry barriers in the Digital Single Market, including for access to media, cultural and educational content.*[11]

Open standards are also essential to allow firms to compete in markets dominated by a monopolist (or oligopoly), with *de facto* standard-setting power. One standards body expert interviewee commented: "of course, the problem is the main

[11] European Commission, ICT Standardisation Priorities for the Digital Single Market, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2016) 176 final, 19 April 2016, p.2.

players are not interested in [standards], because you're basically trying to displace them."

The EU's consolidated Framework Directive on electronic communications networks and services (2002/21/EC) requires Member States to "encourage the use of the standards … for the provision of services, technical interfaces and/or network functions, to the extent strictly necessary to ensure interoperability of services and to improve freedom of choice for users" (§17(2)). It requires the European Commission to publish such standards in the Official Journal of the EU. The Commission may request one of the European standardisation organisations to draw them up, making use of relevant international standards where available; and designate standards as compulsory via the Official Journal.

The European Electronic Communications Code (2018/1972) §61 adds that national regulators may require providers of instant messaging services "to use and implement standards or specifications listed in Article 39(1) or of any other relevant European or international standards." §39 defines European standardisation organisations as the European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation (CENELEC), and European Telecommunications Standards Institute (ETSI)). The international standards bodies mentioned are the International Telecommunication Union (ITU), the European Conference of Postal and Telecommunications Administrations (CEPT), the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

For digital television services, the Framework Directive requires Member States to "encourage proprietors of APIs to make available on fair, reasonable and non-discriminatory terms, and against appropriate remuneration, all such information as is necessary to enable providers of digital interactive television services to provide all services supported by the API in a fully functional form." (§18.2)

The Access Directive (2002/19/EC) allows national regulatory authorities to require operators to "grant open access to technical interfaces, protocols or other key technologies that are indispensable for the interoperability of services or virtual network services", and "to provide access to associated services such as identity, location and presence service" where the authority "considers that denial of access or unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market at the retail level, or would not be in the end-user's interest." (§12)

These Directives, as well as the Regulation on European standardisation (1025/12/EU), mainly related to technical standards specified in public procurement, and Directive on provision of information in the field of technical regulations and of rules on Information Society services (2015/1535/EU), contain detailed standardisation processes that could be drawn upon by the Digital Markets Act and regulators if needed.

In particular, Annex II of the Standardisation Regulation includes relevant conditions on standards body openness, consensus and transparency that could be considered in recognising standards from international non-governmental standards bodies such as the IETF and W3C.

Recognised standards must meet requirements for:

1. Support and maintenance over a long period;
2. Publicly available on reasonable terms;
3. Standards-Essential Patents must be licensed on a Fair, Reasonable and Non-Discriminatory (FRAND) basis;
4. Standards must meet market and regulatory needs;
5. They should be neutral and stable;
6. They should permit multiple competing interoperable implementations, and not be controlled by any other body.

The problem identified with the current approach was identified by a standards body expert interviewee as follows: "The Commission's prime standardiser is ETSI (they founded it after all). So, whatever you may do in the new approach legislation (taking into account standards) will have to be a European norm in the sense of Regulation 1025/2012/EC. And only CEN, CENELEC and ETSI can do this. They use this for bad competition behaviour against other standards bodies. W3C is struggling to integrate its WAI guidelines into the required ETSI Specification EN.301.549 while ETSI tries to take over change control. This is a major legal nightmare." A former official interviewee added: "If ETSI is the answer to any of this, then we need another question. It's slow, captured by commercial interests (who at least compete within ETSI to screw each other over). Although Facebook would hate mandated standards, as a second best I bet it would love ETSI to take the lead. It could pack and delay for years."

A second standards body expert interviewee commented:

> *I tend to have a negative view of those region-specific standards. They are a really hard sell. There are people who have shown interest in implementing those standards, then you have to tell them we are going to have our own version of this. So, I don't know if this is a good strategy. If there was an analysis done and it says, it almost works but we need this and this to be changed… you could argue OK, where does that work happen, it doesn't necessarily have to happen in W3C, although I'm sure they would be happy to do to it. Then maybe ETSI or others could do it. So, the European Commission could be the origin of taking another look at this area. Do the standards we have do enough or does there need to be more? And if we have the will of the major players, we could look at where that work should be done. But none of these systems are regional… So, I*

really don't think this is the right approach. I am really for global standards as much as possible, and I don't think Europe should try to force this issue by creating their own version. They will alienate everyone else. But it's going to take years.

An SME developer interviewee suggested:

We cannot just write a standard or even a specific body in the DMA. You need a process by which the Commission partly has to acknowledge standards, we are now recommending, maybe in future we change. Maybe informal? Or at least a way to tell standards bodies about missing pieces. People at IETF are mostly American so have a very different view of the role of government in general, and have a 90s-style anarchist view, which is fine, but I think is a bit out of date. Even if you tell them there are some public policy objectives in Europe, not US, they say, we don't develop stuff because governments need it, it's a bad sign and maybe something we should not do.

ETSI could be a player. You need something more European. Not a matter of control, a matter of mindset and values. IETF people are great engineers, but see the world in a way that is different from what we see in Europe. So, if you want to get something that meets the European view of horizontal competition or control and govt involvement/representation of the public interest, then you need something not so dominated by Americans and their mindset.

A side-effect of this is we need a better way of promoting a European standards body with IETF-like good things like transparency, but have to make sure it's overseen by Europeans, reflects EU public policy. Public entity, European regulator gives input into the standardisation process of objectives, then checks the standard meets it, then approves/recognises it. But maybe not even necessary.

My feeling is W3C is very similar to IETF, and is even more dominated by the big platforms because it's at the Web level. In the end the point is you should check people do their homework, the requirements you give them as a community. Even with a SWIPO working group (free flow on non-personal data — cloud porting and switching), led by the European Commission, the result is you get big companies interested in making sure nothing happens. Vendors have to declare if they will lock you in – and of course they write it in the small print of the contract.

Institutional support for standardisation

The European Commission's Multi Stakeholder Platform on ICT Standardisation is an expert advisory group, where Member State and Commission representatives meet technical standards bodies four times each year.[12] This would be an ideal venue to plan standardisation support for interoperability requirements in digital markets. A computer scientist interviewee observed:

> *We have to leverage all the standards organisations. The dividing line between IETF and W3C is no longer clear. Pick up the best of what's out there. Question is whether you then say there's a process by which this will be taken forward internationally, or just tell people to use the forum — IETF, W3C where it came from.*
>
> *With CCITT, GSM, classic telco standards, every government gets a seat. This is not true of W3C. National standards institutes and European standards bodies are similar. I can quite see the EU would be reluctant to go down the path of using IETF or W3C. This is also a big problem for developing countries, who don't have private sector firms at the private standards organisations. So, we need processes that are international in scope, including in bringing in other parties (similar to CCITT). The British Standards Institute drives the Commonwealth as member states feel they have a voice.*

One platform engineer interviewed observed: "Standards bodies need to ensure standards can evolve to avoid ossification of functionality. Large companies have a strong incentive to minimise the functionality standardised, and standards organisations need to pre-empt methods of capture, like sending massive numbers of staff to meetings."

A standards body expert interviewee noted: "Standardisation is a very burdensome thing. It's so much nicer where you just do whatever you want. When you come to standards bodies with an idea, you go through the mills of internationalisation, of accessibility, and it becomes infrastructure, and that is not paying off for companies. Privatised infrastructure doesn't work. Company-controlled APIs, there you can move fast, you can outpace your competition. When HTML moved from the W3C, this was mainly kicking out all the accessibility guys… We need a system like the Art. 29 WP or the so-called EU New Approach legislation. To evolve the data formats or protocols or APIs, the law points to an acknowledged specification. If the specification is changed, it needs a new acknowledgment. This worked for

[12] Commission Decision of 28 November 2011 setting up the European multi-stakeholder platform on ICT standardisation, OJ C 349/04, 30 November 2011.

electronic signatures (somewhat) and currently works for accessibility." An SME engineer interviewee added:

> *You don't only need to have a standard interface or protocol, but you also need to define a "set of interoperable features" that are understood, described and implemented coherently across all participating services. This is an easy pitfall for non-developers: non-technical people think that speaking the same language is enough for two parties to work together. But even if both parties speak English, if I insist on calling the bit of audio I send in my message a "vocal message", while you insist on calling it an "audio attachment", especially if we both are machines, we will never understand that we are actually referring to the same thing and thus we will not be able to process each other's communication. This is typically where engineers get crazy and annoying, because an engineer from the first service will passionately insist that "vocal message" is the only correct way of calling it and people that call it "audio attachment" miss the point and are in fact idiots.*
>
> *What you need is not a (protocol) spec, but a dictionary, or more precisely (to make engineers happy) an ontology – a classified description of your world. Actually, the lack of a standard ontology is what keeps most types of technical environments from interoperating; I know of efforts to define one for the IoT space, but we definitely need one for humans – for social activities, identities and personal information. As a minimum, we need to make sure that any regulatory solution for interoperability has a standardisation process that is also capable of producing one.*

As well as regulatory issues, the EU should consider funding support to produce basic software and services to underpin interoperable infrastructure. A computer scientist interviewee suggested: "IETF used to demand two open interoperable implementations before progressing a standard. So, the European Commission should make funding available for that type of advanced development. As part of the process the standards coming forward need this."

A standards body expert interviewee emphasised "there is no European browser. Google or Apple will not allow you to experiment. Google has total control of Chromium. You could fork it. But the maintainer is not paid by Google. If you would inject new ideas into Chromium, they would be rejected by the maintainer, or if you succeed, they will branch, like they did for WebKit. It would cost £10m/year to task the University of Bochum, which is the godfather of Chrome and WebKit, to compete, with European values. Don't allow trackers, you have higher security, TLS done properly. It costs not much and will change interoperability. The Chinese have 16 browsers, some state supported (everything is.) In Chrome you can clearly

exemplify things by showing people the DNT interface. It's almost impossible to find it."

An SME engineer interviewee commented: "As long as you leave things entirely up to 'technical self-regulation', there will be ample opportunities for capture of any process – so you need an independent entity (a regulator) tasked with setting requirements and checking that they are met in results. Then, of course the issue is how do you prevent big business lobbyists from capturing the regulator or the politicians that appoint its board, but at least that's a slightly easier and much better-known problem."

Relatedly, an SME engineer interviewee commented: "what happens in the Web standardisation space is that Google – sometimes with a little push by those revolutionaries at Mozilla – defines which ideas will live and which will die, and how they are to be standardised. All the others – especially, all other non-browser-makers that happen to need something implemented in browsers – basically can only accept what Google decides, or at most make noise in public to create some pressure."

A standards body expert added:

> *IMHO (in my humble opinion), the main obstacle is social dynamics. We had so many nice initiatives on interoperable social networking, DNT etc. This is all simply killed by market power. Large companies will successfully undermine all interoperability unless they have an interest.*
>
> *Microsoft was instrumental in creating Cascading Style Sheets (they thought it could be useful to bring MS Word to the Web I assume). After a successful start, they quit the Working Group, did Internet Explorer 6 (IE6) with JavaScript and halted all development, as IE6 was so dominant they wouldn't have to do anything anymore. The websites had to hack JavaScript and ActiveX and things. It was a mess.*
>
> *Only after the Commission investigation and the very high fines, Microsoft returned to W3C, contributing massively to the making of CSS, which became a very important piece of interoperability of the Web. They changed strategy, that's why it happened IMHO. Not because of the fines.*
>
> *Google just paid the fines and doesn't change strategy. I also think this is strongly related to governments using those proprietary services because it is sooo convenient. As long as this persists, we have no chance whatsoever to decree interoperability on the*

> *current Internet power concentration in a few hands. I would say, currently, the EU is furthering the situation it deplores.*

A free software developer interviewee pointed at the Web Hypertext Application Technology Working Group (WHATWG) as an example of an institutional mechanism for ongoing standardisation, where "browser vendors closely work together with each other to ensure websites work the same in each one. This puts them already way ahead of most other platforms, and perhaps we should be content if we can get every tech platform to this position." However:

> *Although the WHATWG allows any browser vendor to join (see their antitrust agreement), their definition of a "qualifying entity" is narrow and hard to meet, so it's pretty much a cartel of the existing browser vendors (while web publishers and other non-browser stake-holders are left out). Moreover, with Chrome being both the most well-funded and most widely used browser, the power balance among them is rather skewed — and since Google are providing web-based services themselves, and their income is from advertisers rather than browser users, they have significant conflicts of interest.*
>
> *WHATWG's history is also remarkable: as far as I understand, it was formed as browser vendors were unhappy with the W3C's sluggish formalities; they started creating specifications in parallel, provocatively called these "the HTML standard", and by being the 'gatekeepers' to the web they slowly grabbed power from W3C until the latter saved face by cooperating/capitulating.*
>
> *On the positive side again, WHATWG's approach could be considered a welcome innovation in standards making: they create living standards, which are continually updated and lack version numbers, while remaining nearly always backwards compatible with previous versions. Browsers have demonstrated that companies can base software on standards, while still innovating at a high pace. Many business-minded politicians may like that idea. Though personally, I think "innovation" as such is not to be praised; the web's innovations often also help entrench companies' power, while other innovations that would empower users simply do not happen.*

Mozilla and diaspora* developer Dennis Schubert, who has written extensively about standardisation issues with ActivityPub, has suggested: "It does not take much to imagine an ActivityUniverse Standards Foundation, with everyone working on an implementation in the board, the same open submission process, the same open approval workflow, and reliable and complete specification documents in the end. There could have been a very strict base set of things that are absolutely needed, and a set of optional extensions, alongside a mechanism to reliably

discover support for those extensions. Besides, that base set could also address the problem of receiving contents the receiver is not capable of parsing."[13]

Data portability, access and sharing

All of the recent major digital competition reviews have noted the role user data held by platforms can play in helping large online platforms move into new, "adjacent" markets; and can itself act as a barrier to entry to competitors. The UK Competition and Markets Authority (CMA) found in 2020: "Over a third of UK internet users' total time online is spent on sites owned by Google and Facebook. Both companies are also able to gather substantially more data about consumers than their rivals."[14] The UK's Furman review concluded: "The extent to which data are of central importance to the offer but inaccessible to competitors, in terms of volume, velocity or variety, may confer a form of unmatchable advantage on the incumbent business, making successful rivalry less likely."[15]

This data can also be used by platforms to compete with firms making use of their services, with the CMA uncovering evidence "[e]mails between Facebook employees describe concerns expressed by Foursquare, Amazon and Comcast, that data these parties provide to Facebook will ultimately be used by Facebook to compete with their consumer-facing services."[16]

The EU's General Data Protection Regulation (2016/679) already gives Europeans a "data portability" right to demand access to their personal data held by a data controller, where it has been provided by the user or observed from their actions, and is processed on the basis of their consent or for the performance of a contract. (It does *not* cover data inferred about a user, or processed using other legal bases, including the widely used "legitimate interests".) This data should be supplied in a "structured, commonly used and machine-readable format". Users "have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided" (§20(1)). In addition, the user has the right "to have the personal data transmitted directly from one controller to another, where technically feasible" (§20(2)).

Vestager's special advisers, and the German government's "Competition 4.0" report, both focused heavily on "data interoperability" as a mechanism to enable competition. This would be an enhanced version of data portability, enabling real-time access to a larger range of personal data than is covered by the GDPR.

However, one computer scientist interviewee assessed that API/protocol access is more important (and would anyway be required to enable real-time access), with

[13] D Schubert, ActivityPub – Final thoughts, one year later, 31 January 2019.
[14] Online platforms and digital advertising (London: Competition and Markets Authority, 2020), p.42.
[15] J Furman, D Coyle, A Fletcher, D McAuley and P Marsden, Unlocking Digital Competition (London: HM Treasury, 2019), p.34.
[16] CMA, fn 14, Appendix J, p.13.

portability via users "fundamentally useless because of the ability for data to be corrupted. The UK's Open Banking started with data sharing and ended up defining all the APIs, so the user didn't need to touch data. APIs are simply the structured way to get access to the data, and if you want real-time data then you're going to have some publish/subscribe model. It's critical for these things to be usable." Enhanced "data interoperability" would for these reasons likely be more dependent on data transferred directly between two firms at the request of a customer.

An academic review also suggested: "Data portability has been the subject of intense focus by both tech companies and policymakers. However, it may be that the type of data portability that is the focus of those discussions... is simply a poor mechanism to increase competition online. If that is the case, time spent debating specific aspects of a given data portability regime may be better spent considering different types of approaches to competition concerns."[17]

A further, commonly suggested mechanism is to require dominant platforms to share data with competitors. Vestager's special advisers concluded, in "highly concentrated markets with high and non-transitory barriers to entry", with "data-driven feedback loops that tend to further entrench dominance, the benefits for competition and innovation to be expected from a mandated data sharing may then outweigh the negative effects on the dominant firm."[18]

This mechanism will be addressed in much greater detail in the EU's proposed Data Act in 2021,[19] partly because of the difficult data protection issues it raises if individual-level data is shared.[20] However, aggregate statistics are less difficult in this regard. For example, Cave suggested in the case of ride-hailing platforms:

> *the sharing of the data which would be mandated would relate to anonymised data on customer preferences, reflected in transactions data – for example the number of journeys sold between one disaggregated location to another. Such information would allow a rival to direct and locate its vehicles in a fashion which better reflected the overall demand for services, than would be possible using its own information. The largest operator on which this obligation is asymmetrically applied would still have the benefit of knowing the transaction histories and possibly other attributes of individual customers, which would enable them additionally to price-discriminate*

[17] G Nicholas and M Weinberg, Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors? New York University School of Law.
[18] Crémer et al., fn 9, p.105.
[19] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, A European strategy for data, COM/2020/66 final, 19.02.2020.
[20] British Institute of International and Comparative Law, Consultation response to UK Competition and Markets Authority (CMA) Online platforms and digital advertising market study, 11 September 2019, para. 41.

> *among them. But privacy issues will exclude the sharing of such information.*

Vestager's special advisers concluded "there may be a need to oversee that data access is granted on fair, reasonable and non-discriminatory (FRAND) terms – which need to be specified case by case. Very likely, mandated data access will therefore, in the end, be a sector-specific regime, subject to some sort of regulation and regulatory oversight. Nonetheless, competition law can specify the general preconditions and give a more fundamental, pro-competitive orientation to the regulatory regimes that are likely to arise."[21]

Where individual-level data sharing is required under EU competition law, an institutional mechanism to protect privacy is to require the approval of the national data protection authority. A French example of this is the Autorité de la Concurrence *Énergie* decision, which required CNIL approval of data sharing provisions.[22]

A complementary route to limiting the anticompetitive effect of the collection of detailed information about large numbers of users by dominant platforms is exemplified by the German Federal Cartel Office's (BKA) 2019 decision against Facebook:

> *The authority holds that Facebook is the dominant company in the national market for the provision of social networks. The company abuses this position by, contrary to the rules of the General Data Protection Regulation (GDPR), making the private use of the network dependent on the authorisation to link the data relating to users and their devices generated outside facebook.com with the personal data generated by the use of Facebook itself without additional consent given by users.*

This decision was upheld in an interim decision by the Federal Court of Justice in June 2020. The BKA summarised the ruling as emphasising "terms of service are abusive if they deprive private Facebook users of any choice as to whether they wish to use the network in a more personalised way linking the user experience to Facebook's potentially unlimited access to characteristics also relating to the users' 'off-Facebook' use of the internet; or as to whether they want to agree to a level of personalisation which is based on data they themselves share on facebook.com."[23]

In a commentary on the decision, Prof. Rupprecht Podszun added: "If the dominant market player collects more and more data from users, chances for actual or

[21] Crémer et al., fn 9, p.109.
[22] Autorité de la concurrence, Décision n° 17-D-06 du 21 mars 2017 relative à des pratiques mises en œuvre dans le secteur de la fourniture de gaz naturel, d'électricité et de services énergétiques.
[23] Bundeskartellamt, Federal Court of Justice provisionally confirms allegation of Facebook abusing dominant position, 23 June 2020.

potential competitors are lower and market entry barriers are raised. You can no longer compete for advertising contracts in the same way or for a social network experience."[24]

Personal Information Management Systems (PIMS) and Personal Data Stores

Personal Information Management Systems (PIMS) and Personal Data Stores (PDS) are two technical mechanisms proposed to improve the portability and interoperability of systems using personal data. This should reduce switching costs and make multi-homing easier.

A PIMS gives a user the ability to manage all of their personal data, wherever it is stored, using standardised protocols and schemas to communicate with the

[24] R Podszun, Facebook Case: The Reasoning, 28 August 2020.

systems holding the data. With an understanding of the meaning of that data, users can query it in a unified way, for example asking for a recommendation for a business lunch location based on all of the user's previous lunch spots, today's weather, and any special offers available. The data may be held in one location controlled by the user, or queried directly with service providers.[25]

A Personal Data Store lets a user store all their own personal data, whether on a device they directly control, or a remote service where the data is protected using encryption and related technical measures. The user may then authorise other services they wish to use to interact with their own data store remotely. Solid is one project developing such tools, co-founded by the inventor of the Web, Tim Berners-Lee.[26] In some implementations, such as Databox, those services send software to the PDS, to run in a protected "sandbox" environment, which means the service provider never needs to access the data directly itself, thus enabling very high levels of protection for even very sensitive information.[27] The "Small Web" project is developing tools for users to manage all their data and services using devices they control in a peer-to-peer network, connected to the centralised Web.[28]

A review by the UK's Competition and Markets Authority identified the following potential benefits of PIMS and PDS:

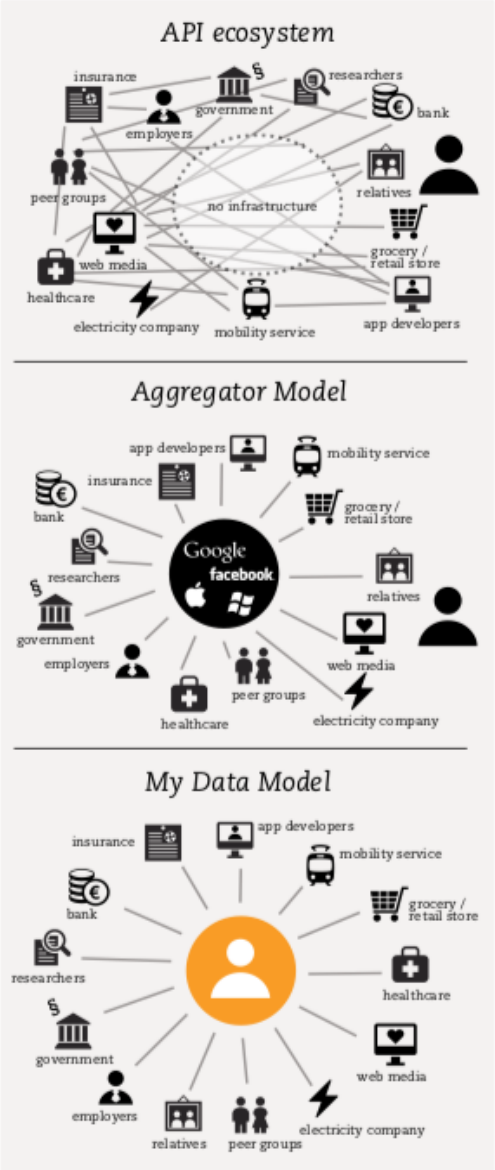


Figure 4 The MyData model

1. Enable individuals to track all the users of their personal data (data controllers, in GDPR terms), and exercise their GDPR rights – e.g. manage and revoke

[25] J Kramer, P Sennellart and A de Streel, Making Data Portability More Effective for the Digital Economy: Economic Implications and Regulatory Challenges, CERRE, June 2020, p.45.
[26] See https://solidproject.org/team
[27] Y Zhao, H Haddadi, S Skillman, S Enshaeifar and P Barnaghi (2020) Privacy-preserving Activity and Health Monitoring on Databox, In 3rd International Workshop on Edge Systems, Analytics and Networking (EdgeSys '20), April 27, 2020, Heraklion, Greece.
[28] See https://small-tech.org/research-and-development/

consent for specific uses, make subject access and portability requests, object to certain processing, and to erase data.

2. Act as identity providers, enabling an individual to login to many different websites while protecting their privacy.
3. Keep secure backups of users' personal data.
4. Facilitate micropayments for services that require it, in addition or as an alternative to providing access to personal data for advertising and other purposes.[29]

The CMA also concluded "inferred or derived data is an important factor contributing to the market power or SMS of the major platforms. Consequently, if the data sharing requirements of GDPR do not extend to derived or inferred information it may not be adequate to address our concerns."[30]

These types of mechanisms have worked well in the UK's Open Banking programme. The CMA found their practicability will "hinge on their commercial viability arising from consumers' incentive to adopt them rather than their technical feasibility. That said, to work reliably such remedies may require a lot of investment in technology, including in the ancillary measures needed to support them."[31] These include building consumer trust in potentially unfamiliar services.

As with all multi-sided markets, "a prospective PIM provider would still face a difficult 'chicken and egg' problem: consumers would be unlikely to sign up unless advertiser-funded incentives were available but advertisers would be unlikely to use a PIMS until sufficient customers had joined."[32] And these cross-side network effects would tend to result in winner-takes-most dynamics, so further measures would be needed to prevent PIMS becoming a competitive bottleneck.[33]

The Finnish government has supported the development of a MyData framework implementing a personal information management system, shown in Figure 4. The framework principles are shown in Table 1.[34]

[29] Competition and Markets Authority, Online Platforms and Digital Advertising Market Study Interim Report, Appendix L: Potential approaches to improving personal data mobility, 18 December 2019, p.L3.
[30] CMA, fn 14, Appendix L, p.12.
[31] CMA, fn 14, Appendix L, p.14.
[32] CMA, fn 14, Appendix L, p.16.
[33] CMA, fn 14, Appendix L, p.19.
[34] A Poikola, K Kuikkaniemi and H Honko, MyData – A Nordic Model for human-centered personal data management and processing, Finnish Ministry of Transport and Communications, undated, ISBN: 978-952-243-455-5.

1. Human centric control and privacy: Individuals are empowered actors, not passive targets, in the management of their personal lives both online and offline – they have the right and practical means to manage their data and privacy.
2. Usable data: It is essential that personal data is technically easy to access and use – it is accessible in machine readable open formats via secure, standardized APIs (Application Programming Interfaces). MyData is a way to convert data from closed silos into an important, reusable resource. It can be used to create new services which help individuals to manage their lives. The providers of these services can create new business models and economic growth to the society.
3. Open business environment: Shared MyData infrastructure enables decentralized management of personal data, improves interoperability, makes it easier for companies to comply with tightening data protection regulations, and allows individuals to change service providers without proprietary data lock-ins.

Table 1: The MyData framework principles.

Figure 4 shows MyData's visualisation of the benefit of a human-centric data mode, helping individuals understand all the organisations they share data with, and helping organisations "manage their API integrations... In the long run, some systemic restructuring will be a necessity." It also helps individuals to easily switch between competing services, enabling data to be used for new purposes, while maintaining effective control of these relationships.[35]

There are now national MyData hubs in 40 countries, with nearly 100 organisational members of MyData Global.[36]

A computer scientist interviewee suggested:

> *PIMS should be like password managers, that's it. By all means keep a copy of data in the cloud, but it only gets decrypted on my device, with policies such as trust this computer, it doesn't need to be unlocked more than once every few weeks. This avoids much standard criminality. In some cases, data controllers will only need to keep it for a few seconds.*
>
> *For IoT it's vital for performance and resilience. Burglar alarms and heating systems rely on smart tech. When the Internet goes down, they need to keep working. In the UK, when the power goes off,*

[35] Poikola et al, p.5.
[36] See https://mydata.org

burglar alarms are required by BSI to continue for four hours, and must be able to independently raise the alarm, e.g. flash a light. But the determination of an alarm condition can't depend on connectivity. In a fire, the power will go off, hence batteries in all these things. Then you get into vulnerable groups, e.g. the elderly, systems must continue working. We're building a world in which we're not sufficiently resilient. Norwegian rural communities require homes to have independent heating for seven days, e.g. a wood burner and two tonnes of wood.

*But nobody can be bothered to download data from controllers and put them in PDS. No-one can be bothered, it's f***ing useless. The UK midata initiative, when they told the energy companies what they needed under this scheme, it was less data than already being voluntarily provided. Lots of valuable data got lost as they didn't consult people who understood the real value in the data (and its fidelity.) I wish smart meters had Ethernet jacks or serial lines, then you could use them at a highly granular level at home. There's no value to companies to carry and store that detail of data. Apps could be written that could do behavioural change in how I use energy. Low-power efficient appliances. Actionable intelligence. But it has to be that when you — PayPal is sort of trying to do this — login with PayPal and we'll get all your details, like delivery address. That simple model of you can get all my data from here, here's my OpenID, these are the fields you want, only keep them x days (needs enforcement) — that's about defining what are the interoperable protocols for those things, not expecting manual import of data.*

Device neutrality

The French telecommunications regulator ARCEP has noted that while the EU (and other jurisdictions) has an extensive "network neutrality" regulatory regime,[37] which protects the "Open Internet" provided by Internet Access Providers (the lower layers of the "iceberg"[38] shown in Figure 5), this regime does not extend to devices used to access Internet services – whether PCs, laptops, smartphones, or Internet of Things devices such as smart speakers, watchers, lights, heating systems or many others (largely covered by the top two layers of the "iceberg".)[39]

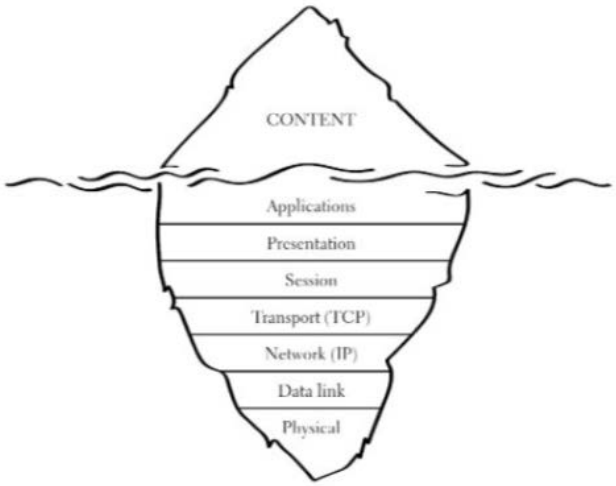


Figure 5 Brown and Marsden's "iceberg" model of Internet regulation

Providers and operators of such services "may be induced to negotiate preferred placement and functionality on devices, or may be disadvantaged in comparison to the apps of vertically integrated providers. For example, apps of vertically integrated providers [such as Apple, Microsoft or Google] may be placed more prominently or may be easier to access, may not be as easy to uninstall, or may have privileged access to hardware, such as battery management, or built-in sensors and chips (e.g. NFC, GPS, Bluetooth)."[40]

In this vein, the European Commission is already investigating Apple's restriction of access to its iPhone's secure chip for payment apps from other providers (potential abuse of dominance under TFEU §102), and terms for integration of Pay into

[37] The so-called "Open Internet Regulation" (2015/2120).
[38] I Brown and C Marsden, Regulating Code (Cambridge: MIT Press, 2013) p.8.
[39] Autorité de régulation des communications électroniques et des postes, Devices, the weak link in achieving an open internet, February 2018.
[40] J Krämer, Device neutrality: the missing link for fair and transparent online competition? Centre on Regulation in Europe Issue Paper, March 2019, p.3.

merchant websites and apps (potential anti-competitive contracts under TFEU §101),[41] and has opened a sector investigation into the consumer Internet of Things.[42]

Krämer identified the following opportunities for discriminatory conduct by firms controlling device hardware; operating system; web browser; and app store:[43]

A firm controlling the hardware level could: • privilege, restrict or prohibit access to certain networks (mobile, ad-hoc or infrastructure networks); • prohibit or inhibit the installation of certain operating systems; • reserve or privilege system resources (e.g. battery, memory, computing power, storage, dedicated interfaces) for specific apps; • prohibit, inhibit or restrict software at higher layers from accessing hardware components (e.g. sensors, chips, camera, microphone); • prohibit, inhibit or restrict compatibility with ancillary hardware components and devices.	A firm controlling the operating system level could: • privilege, restrict or prohibit access to certain networks (mobile, ad-hoc or infrastructure networks); • prohibit or inhibit the installation of the operating system on certain hardware; • reserve or privilege system resources (e.g. battery, memory, computing power, (data) storage) for specific apps; • privilege, prohibit, inhibit or restrict software at higher layers from accessing hardware components (e.g. sensors, chips, camera, microphone, screen); • prohibit, inhibit or restrict compatibility with certain applications and devices; • pre-install certain applications and restrict removal of some or all of these applications; • integrate certain applications more tightly in the operating system and user workflow (e.g., voice and zero-click activation, background performance, notifications).
A firm controlling the browser could: • privilege, restrict or prohibit access to selective content (e.g., block	A firm controlling the app store could: • deny, unduly delay or discriminate access to the app store based on (legal)

[41] European Commission, Antitrust: Commission opens investigation into Apple practices regarding Apple Pay, 16 June 2020. Case number: AT.40452.
[42] European Commission, Antitrust: Commission launches sector inquiry into the consumer Internet of Things (IoT), 16 June 2020.
[43] Krämer, fn 40, p.8.

advertisements, set default starting page and default search engine); • privilege, restrict or prohibit access to selective plug-ins/extensions; • bias, distort or restrict "reachability" of certain websites or plug-ins based on (legal) content, functionality or identity of the website owner (e.g., discriminate with respect to the loading speed of certain websites, warning messages). • privilege, restrict or prohibit websites' or plug-ins access to the browser's full functionality (e.g., JavaScript, service worker, stored data); • prohibit or inhibit its installation on certain operating systems; • reserve or privilege system resources (e.g. battery, memory, computing power, storage) to specific content; • unduly delay or omit the adoption of web standards (e.g. in order to retain control over functionality reserved for native apps, especially if the firm controls the app store level as well).	app content, app functionality or identity of the app developer; • bias, distort or restrict "findability" of certain apps based on (legal) app content, app functionality or identity of the app developer. • require or prohibit apps to use ancillary services and functionalities (e.g. payment services, push notifications, reporting services) • require apps to share data or deny access to data in a discriminatory way; • prohibit or inhibit its installation on certain operating systems or devices.

Table 2. Examples of possible device neutrality issues (Krämer, 2019)

The EU's so-called Platform-to-Business Regulation (P2BR)[44] contains transparency provisions for operators of "Online Intermediation Services", and notes in Recital 30:

> *it is important that the provider of online intermediation services acts in a transparent manner and provides an appropriate description of, and sets out the considerations for any differentiated treatment, whether through legal, commercial or technical means, such as functionalities involving operating systems that it might give in*

[44] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ L 186, 11.7.2019, p. 57–79.

> *respect of goods or services it offers itself compared to those offered by business users. To ensure proportionality, this obligation should apply at the level of the overall online intermediation services, rather than at the level of individual goods or services offered through those services.*

However, unlike the Open Internet Regulation, P2BR does not prohibit discriminatory treatment.

While the European Parliament pushed for P2BR to include operating systems, it is not covered by the final Regulation. However, the first review by the European Commission, scheduled for January 2022, must assess "the effect of this Regulation on any possible imbalances in the relationships between providers of operating systems and their business users" (§18(2)(e)).

A significant policy question is the extent to which device neutrality as such – if judged important by policymakers – should be implemented as a specific regulatory category, perhaps within the Open Internet Regulation framework; as part of the regulation of large online platforms in the Digital Markets Act; and/or using existing powers under the broad EU competition regime. But a workshop organised to consider this question, featuring a keynote from the director of ARCEP, found "general agreement that we should be very careful when contemplating the possibility of applying neutrality and non-discrimination rules to device manufacturers and their integrated [operating systems]."[45]

Many of the competition issues raised relating to devices are similar to those with Internet Access Services, and other large online platforms. However, as Krämer notes, they have been judged by the EU to be significant enough to deserve specific regulation. And in traditional competition terms, "enshrined dominant positions and termination monopolies (e.g., due to the fact that devices can be very expensive and consumers use them for an extended period of time) may well exist in the context of devices, and operating systems, as well as their associated (software and hardware) ecosystems."[46]

Open identities

The Internet Engineering Task Force's (IETF) OAuth 2.0 protocol allows a user to securely authorise a third-party service to access resources belonging to their account on another platform, rather than having to share passwords or other security-critical information with such services.[47] It is widely used by sites, including Twitter, to enable access by complementary services, to a user that already has an account on that platform (shown also in Figure 6). It can also be used by a

[45] Centre on Regulation in Europe, Device Neutrality: Issues and Policy Options, 21 March 2019, p.2.
[46] Krämer, fn 40, p.9.
[47] See the website about the protocol maintained by Aaron Parecki.

substitute service where a user already has an account with the original platform and wishes to multi-home.

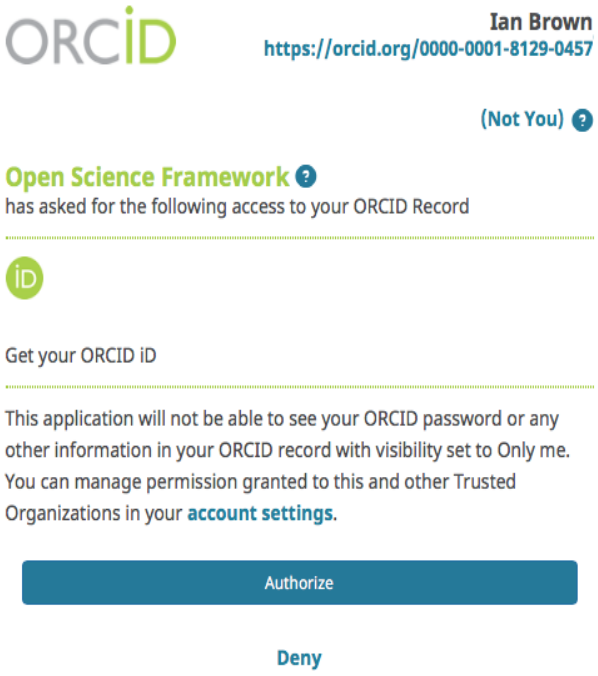


Figure 6 Using OpenID to login to LawArXiv

Where a third-party service wishes to access a platform where a user does not have an account – for example, because they are unwilling to accept advertising-focused behavioural profiling – additional user information will be required. For example, if a user Alice on a competitor social media service wished to share content with her friend Bob on an interoperable Facebook, they would first have to become "friends" – meaning Alice's service would have to send a "friend" request to Facebook, with enough information for Bob to decide whether to accept the request next time he used Facebook. The ActivityPub protocol includes a "Person" object, which could include information to help Bob make this decision.

Additional functionality would be possible using OpenID Connect,[48] which is built on OAuth 2.0, and is used for example to enable Google Sign-In across platforms (see the example in Figure 7). More complex functionality is possible using the Kantara User Managed Access protocol; W3C's Verifiable Credentials and Decentralized Identifiers; and IndieAuth.

[48] See https://openid.net/connect/

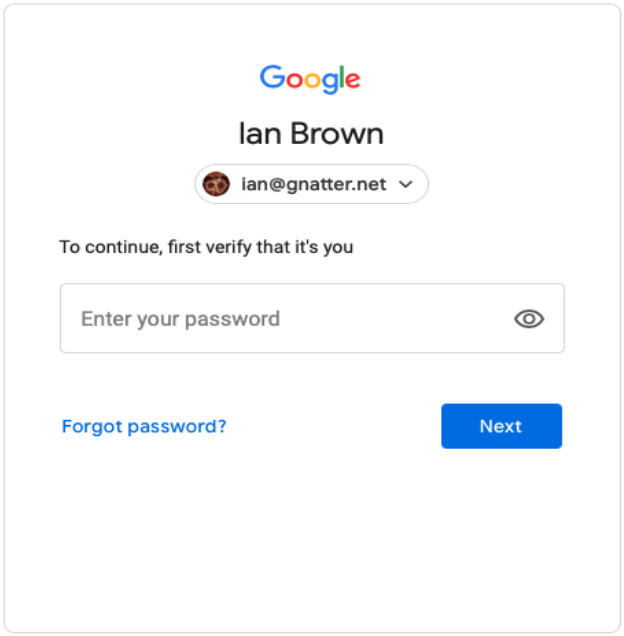


Figure 7 Logging in using a Google ID and the OpenID Connect protocol

These "open identities" are also important for users that wish to take advantage of single-sign on solutions to third-party services, with extra security features (such as multi-factor authentication), but without sharing so much information with the platforms (principally Facebook and Google) that currently provide the most widely-accepted single sign-on features. A computer scientist interviewee suggested:

> *Firms such as PayPal can also supply enhanced identity checks as financial infrastructure. There needs to be a means by which approved verifiers are certified as known good agents who are willing to be audited, not fly-by-nights. Sites will say we support these after passing checks – reputable providers. And PayPal is currently one. (Experian might be another.) We need to standardise around that. My identity provider is my PIMS/PDS. The reason to come back to other providers who essentially – I don't use my password manager for using all my data, but you can't get to my encrypted cloud data with using it – so that's where your IoT data, photos, etc. are.*

A further feature that might become more popular over time where state-backed proofs of identity are required – with a well-developed governance framework – is

the EU's electronic identification and trust services (eIDAS) framework.[49] This currently focuses on ensuring public administrations in the EU's 27 Member States will accept state-backed digital proof of identity on the same basis as their own. The framework also "creates an European internal market for Trust Services – namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication – by ensuring that they will work across borders and have the same legal status as their traditional paper based equivalents."[50]

A European Commission consultation closing in October 2020 asks if eIDAS "should be extended to provide a level playing field for the private economic actors operating in the field of electronic identification."[51] This could provide another mechanism by which EU countries could increase the interoperability of identity technologies. The consultation also asks respondents about the importance of "a secure single digital ID that could serve for all online services (both public and private) that provides you with the control over the use of your personal data". While a single ID is not essential for this purpose, such an extended eIDAS framework could provide practical improvements in the abilities of individuals to use Personal Information Management Systems.

However, an SME developer interviewee noted: "eIDAS is extremely complex and extremely bureaucratic, targeted to extremely secure and public identities, paying taxes, banks etc. and on the other hand platforms have things very simple, you click and you login, with just about whatever information you want to share. That's the use case that is missing. 10% is highly authenticated, 90% is logging into random websites. The standards are there – whoever implements this kind of simple login needs to support any provider, not just Google/Facebook (and now Apple.) Should do the same with open IDs."

A standards body expert interviewee noted:

> *The problem is the identity space is one of the worst when it comes to standards because there are so many. We have the sovereign ID stuff going on and it's yet another type of identity.*
>
> *These systems have to be flexible enough to accommodate different identity systems. Maybe you could settle on a basic default one you could rely on, it has to be open, to be able to evolve. In ActivityPub that's left open. Of course, it leverages the Web and URLs, it's more OpenID kind of thing, but at the data format level it doesn't*

[49] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257/73, 28.08.2014.
[50] European Commission, Trust Services and Electronic identification (eID), undated.
[51] European Commission, eIDAS Open Public Consultation, 24 July 2020.

define what ID string means. And I think it's good it stops there in a way. Imposing one particular standard.

Can interoperability requirements be introduced gradually or in stages?

Scope of interoperability obligations

As a pro-competition measure, interoperability is most appropriately targeted at the largest platforms. This also ensures associated costs of coordination and implementation are not placed on small companies,[52] which maintain their full capacity to innovate by avoiding any homogenising effect from standardisation of core functionality.[53]

While there are universal service arguments for a broader requirement, protecting individuals' ability to switch between several different messaging services reduces the exclusionary impact of closed services. An SME developer interviewee noted: "it would be good if everyone participating in a strategic market (e.g. messaging) would be required to interoperate, but in political terms that might look too much of a state intervention into competition, while it looks politically possible to get something established if it only applies to the big dominant platforms."

That said, a computer scientist interviewee noted: "Nearly all startup systems start inter-operable, it's only when they get large enough that they start playing this anti-interoperability game. They may not switch it on, but many of them start with completely interoperable systems in the first place. It's a design decision by them not to do it, for the purposes of trying to become the next monopoly. Don't require it of every startup, but it will be an emergent property anyway."

A data governance expert interviewee added: "For social media, impose requirements based on number of accounts/size of customer base. Think about cost burden — we can estimate how much it would cost to implement something. That's a reasonable burden for what sized/scaled firm? In telecoms, with local loop unbundling, and with Open Banking, businesses are very good at putting other costs into the regulation bucket. So, do it independently, as well as asking individual firms for issues they don't know about. (UK telecoms regulator) Ofcom has good experience with that, as do other telecoms regulators."

For the major platforms, one standards body expert interviewee noted:

[52] Swire & Lagos, 2013, pp. 350-358.
[53] Kerber and Schweitzer, fn 4, p.42.

> *Facebook could certainly do some of the things they do with ActivityPub and ActivityStreams, it is designed for this. Look at the documentation, use cases and requirements. It's pretty obvious. Nobody was inventing anything new there. How do you post a photo with text, let people subscribe to your feed, notifications when you have posted…? That's the very root of all these services. Publish + subscription + notification. All of that is built into that standard, you already have that. ActivityStreams is kind of open-ended, there is a basic format, then a set of open-ended categories, so you can extend quite a bit. Some people criticised that, they said it's too open-ended, but the W3C working group said you can't possibly plan for every use, you have to make the standards open enough. If you make it too strict people are going to break it. But too open works against interoperability, because people use this extension mechanism. There is a lot that can be done with those standards for sure. Facebook and Twitter engineers could probably do a very quick analysis and figure out what is missing. Give an engineer a problem and they will solve it. If they are interested there is no problem.*
>
> *People who have been implementing the W3C standards typically connect their systems with Facebook and/or Twitter (holding their nose!) so that posts made using their systems are also accessible by Facebook and Twitter users. The very fact that they can thus bridge those systems together actually demonstrates it is possible to have some level of interoperability using the existing standards.*

An SME engineer interviewee noted: "What is possible today is to deal with the two platforms. The theory would say, you could imagine there is just one open standard, everyone uses that. But it's true this can stifle innovation and demotivate people from starting up new companies. You have to discuss whether the threshold is very high, very low – just start with the very biggest platforms, learn by doing… then extend e.g. if you find companies are staying just below the threshold. It's more important you have a mechanism to identify and promptly new platforms and services that meet the threshold. You need a way to add new ones to the list. You need a process."

Effective interoperability requirements also depend on the wider legal framework being enforced. A standards body interviewee expert noted, in regard to the W3C's Do Not Track standard:

> *The W3C process has proven to work well, even under pressure. So, it is not the process, but the outside economic framework and strategies that will kill such work. Its specification work is free, stakeholder driven and not mandatory. ALL privacy efforts in standardisation failed, because the stakeholders (implementers) abandoned it. And no government was there to replace them.*

> *The system that always worked was the US threatening legislation and the GAFAM going to Washington saying self-regulation is far better and they will do something in W3C. And they did. Until the precise moment when the threat of legislation vanished (senator changed mind, abandoned, etc.) The next day, the room was empty.*
>
> *There is no real data protection enforcement in Europe. As there is not a solution by technology produced, there is no incentive to produce such a solution. It is MUCH cheaper to send the lawyers to Brussels and kill the law or digress the effort to something like cookie-banners.*

Expert views on a "minimum standard" of interoperability

We asked all technical interviewees if there is a consensus among experts in this field regarding a "minimum standard" of interoperability; if so, what elements from the full menu are the necessary ones and why? The open-ended suggestions were APIs/protocols, data access/sharing, device neutrality, and open IDs.

All agreed that open APIs/protocols were *the* essential element.

An SME engineer interviewee suggested: "These options are different aspects of the same thing. In general, there is more openness and more, different people working together. And there are different ways openness can be thwarted, including in devices. Today's tech is made of multiple platforms, hardware/operating system/browser/platform e.g. social media. So multiple application layers one above the other, and you need to prevent companies turning them into silos" (as discussed above in the device neutrality section.) S/he added: "The business model for the last decade, according to strategists, is: 'you need to become a platform, make it closed, and make lots of money'. Open identities are one, key technological route to lots of other services: social media; any platform, any two-sided market."

One platform engineer interviewee suggested regulators should ask: "What gives large platforms ongoing infrastructural power that will block entry?"

Practical consequences of interoperability obligations for dominant platforms

The digital competition reviews that examined interoperability in detail – particularly the UK Competition and Markets' Authority (CMA) market study,[54] and the French Conseil national du numérique (CNNum) interoperability study[55] – came to

[54] CMA, fn 14.

[55] Conseil national du numérique, fn 8.

similar conclusions on the practical consequences of introducing interoperability obligations for dominant platforms, in terms of which functions and services would be covered, and what would be accessible, to whom, under which conditions.

Building on these reviews, our interviews, and Marsden's Beaufort scale of co-regulation,[56] we have developed a Fujita scale[57] of interoperability regulation, as follows. It begins at level 0 with the *status quo*, which is largely in the self-interest of platforms (although the CMA noted Facebook "degraded this functionality, the 'Publish actions' API, in August 2018"[58]).

Moving up the scale, in terms of regulatory obligations on covered platforms, gives users more freedom in terms of the services and software they can use to interact with those platforms and their users, but may require increasing levels of regulatory action/market intervention and technical complexity, with transitions from platformed-permissioned->permission-less connection; read->write access to resources; public->private sharing and authorised resource access (particularly the user's "social graph", or contact list); and linkage to own->others' accounts:[59] It might be appropriate to impose the lower level obligations on firms with a substantial market share, while the higher levels would be more appropriate for dominant or "gatekeeper" firms.

1. *Platform-permissioned vertical interoperability*: users can connect their own account on complementary services from a third party to a platform, with its express permission and using its own API or protocol; and use major platform IDs to log in to other services. The platform must technically enable services to connect, through an API key, App Store, or similar mechanism (e.g. Facebook and Twitter, and iOS/iPadOS/watchOS, with their single App Stores where apps must be approved by Apple).

   This level includes *cross-posting* (highlighted by CNNum and the CMA): a platform user can post/share content from complementary services in their feeds.

   Regulators may still wish to impose obligations on platforms regarding public API transparency, competitor/user feedback, and stability, as well as consider any degree of preference (such as search result placement or privileged API access) the platform gives its own non-core services. Platforms could also be required to support common APIs/protocols, such as an updated Do Not Track signal, Open ID protocols, and to enable users to

[56] C Marsden, Internet Co-Regulation (Cambridge University Press, 2011), p.227.
[57] This measures tornado intensity. See TT Fujita (1971) Proposed characterization of tornadoes and hurricanes by area and intensity. Chicago: University of Chicago.
[58] CMA, fn 14, Appendix W, p.10.
[59] It would be more precise to consider this a multidimensional space, with some binary axes such as public/private, permissioned, read/write, linkage to own/others' accounts, access to contacts/"social graph", and scalars such as technical complexity/completeness and market impact.

delegate their privacy and other settings to a third party (such as a consumer protection group). Regulators may consider requiring platforms to enable complementary services to cross-post in the same format as the platform's own services (a pointed noted by the CMA).

2. *Open vertical interoperability*: users can connect their own accounts and open IDs on complementary services, or apps, from a third party, to the core functionality of a platform, without the platform's permission (e.g. software on almost all operating systems on personal computers, and Android smartphones, where alternative app stores are available.) This would enable *real-time data portability*.
3. *Public horizontal interaction* (no external user authorisation needed):
    a) *Publication* – Platforms make content in public feeds (e.g. tweets from non-locked accounts, or public posts on Facebook) available using open protocols, such as Really Simple Syndication (RSS), allowing anyone to access them with any service or app supporting those protocols (such as Feedly), even without an account on those platforms. This is recommended for social media by the French CNNum.
    b) *Messaging* – Platform users can receive messages and other types of content from any other user that can uniquely identify them, on any other service (e.g. e-mail and telephone calls; and most instant messaging systems, which don't require contacts to be explicitly authorised.)
4. *Private horizontal interaction* (external user authorisation needed at this and higher levels): As with the previous level, but with a security mechanism to enable:
    a) *Sharing* – Platform users can share resources (such as a feed) with a limited number of readers (who should not need an account on that platform).
    b) *Messaging* – an account owner can authorise any other user to send them (or groups they administer) messages or other types of content.

    This could be simply a secret URI (Universal Resource Identifier, like a web address) or similar, or a password shared with authorised user(s), with content protected using Transport Layer Security or equivalent. More secure and user-friendly mechanisms could be built using an authorisation protocol (such as OAuth) and open identity protocols.
    c) *Social graph*: a platform user can authorise a third-party service to access enough details of their contact list to identify contacts present on both, and send connection requests to those contacts on the external service, without enabling "spamming" or revealing contact

details without users' explicit consent. The importance of this was noted by CNNum and the CMA.[60]

5. *Seamless horizontal interoperability*: users have the ability to use directly competing services to a platform's own and receive a high degree of compatibility, for:

    a) *Componentisation* – to replace components on a platform, including substitutes for the platform's own services and user interfaces (such as a default browser, search engine or e-mail app on a smartphone OS, or a feed reader or content recommendation and curation algorithm on a social media platform, or a specialised search provider in a general search engine, or a payment service or app store in a broad platform ecosystem such as Google's Android and Apple's iOS/macOS, or digital TV set-top box services). Depending on the service and platform design, this can be the most technically complex requirement. To a significant degree, competition regulators have imposed this on mainstream operating systems such as Windows through enforcement actions in the 1990s, and more recently in the EU case on Google Shopping, although to less approval of competitors.

    b) *Seamless interaction* with its users. Platform users can be contacts with users of other services, and connect their own accounts on other services, while seamlessly communicating and sharing resources using the core functionality of both services. This has the greatest impact on reducing network effects as barriers to entry, and is recommended for instant messaging by the French CNNum.

A mock-up user interface of a fully interoperable social media platform, by the UK CMA (which, like the CNNum, calls this *content interoperability*[61]), is shown in

[60] The CMA concluded: "tools that make it easier for consumers to access their existing networks across multiple platforms could make new or smaller platforms more attractive to consumers and could reduce the extent to which same-side network effects act as a barrier to expansion in the social media sector, Therefore, interventions that extend the availability of these tools, or that limit the ability of incumbents to degrade or withdraw access to them, should help promote competition and benefit consumers." See CMA, fn 14, Appendix W, p.9.

[61] The CMA concluded: "in the long term this measure has the potential to be the most effective model and form of interoperability intervention for overcoming network effects as consumers would no longer need to access a particular platform with a large social graph and network, such as Facebook, in order to engage with users of that platform. However, we recognise the risks associated with this intervention particularly in the form of homogenisation of services and reduced innovation and the need for more extensive regulatory design, as well as the lack of support from existing market participants." See CMA, fn 14, Appendix W, p.18.

Figure 8, with a user on a hypothetical social media platform "Huddlr" connected to other users on Facebook, Instagram, Twitter and Blogspot:[62]

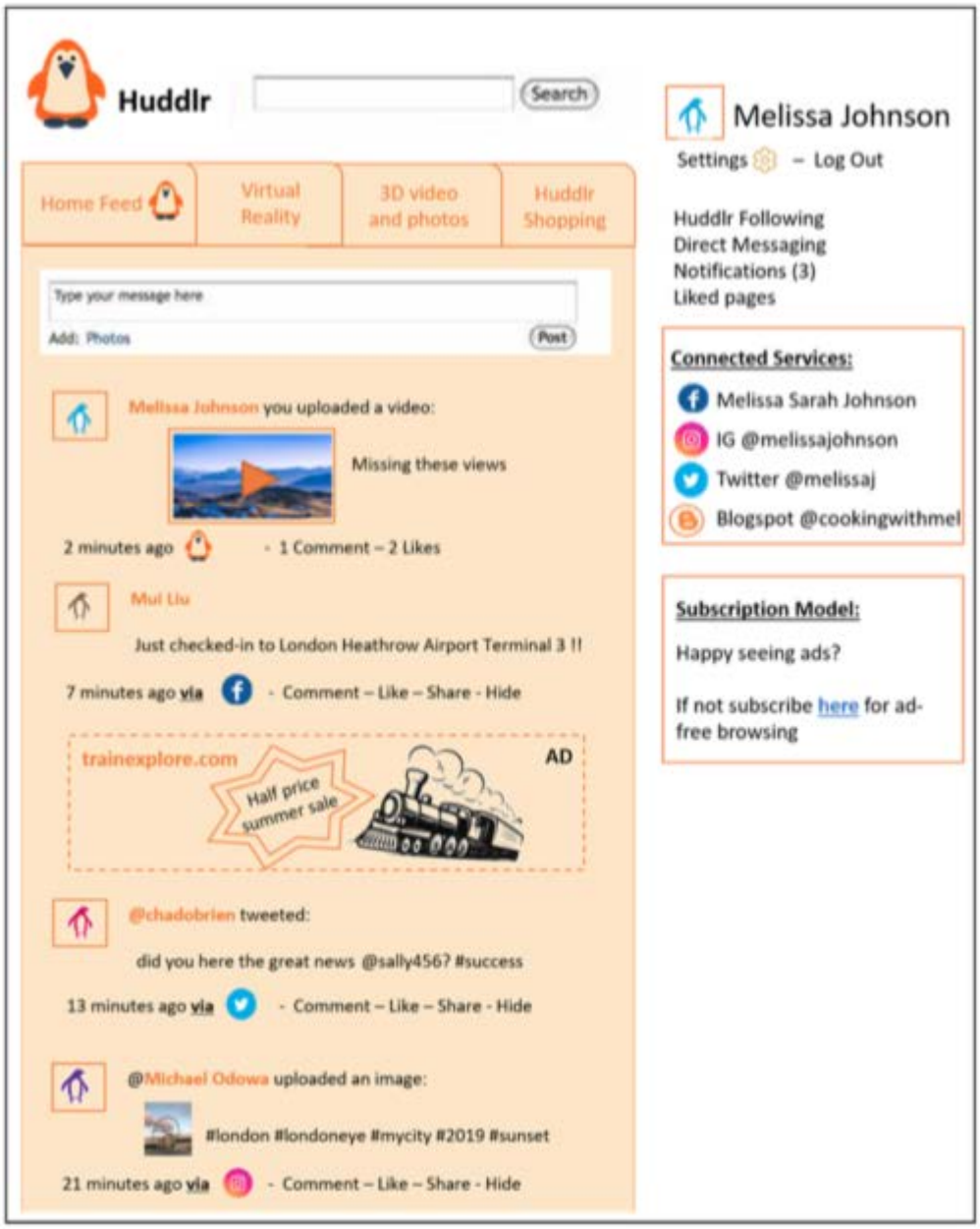


Figure 8 CMA mock-up of an interoperable social media platform

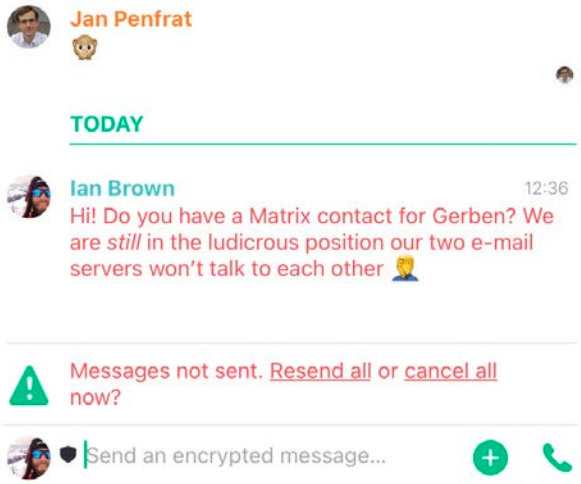
[62] CMA, fn 14, p.373.

Validation mechanisms

An important additional mechanism to make interoperability work well for users is institutional support to verify different companies' systems meet basic standards, as for example the UK's Open Banking implementation entity carries out, with its July 2020 statistics[63] shown in Figure 9:

Figure 9 UK Open Banking compliance testing results for July 2020

Without such verification, incompatible software and/or systems can frustrate interoperability in practice. Figure 10 shows the author's experience with e-mail interoperability, caused by a complex interaction of IPv6 addresses for individually operated mail servers and Spamhaus spam detection based on IPv6 address ranges (which took months to resolve), combined with momentary problems with Matrix's (supposedly) interoperable secure messaging capabilities:



[63] Open Banking Implementation Entity, API performance, July 2020.

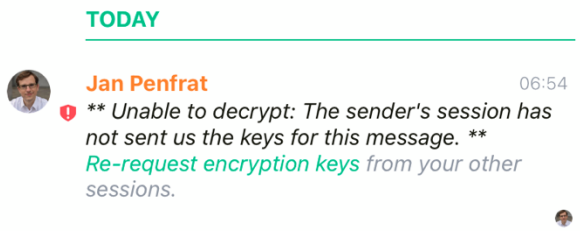


Figure 10 Problems with e-mail and messaging interoperability

A free software developer interviewee added: "A standard should be accompanied by validation tools, and parties implementing the standard must demonstrate its compatibility, as well as document what (parts of) standards they exactly support and since and until what version/date. To avoid the development of standards stalling because companies could not recoup the investment, public money could be made available to facilitate development of standards, research, testing suites, reference implementations, and free software modules that help adopt it."

Restrictions on use of interoperability mechanisms

One of the main objections raised to interoperability mechanisms is their impact on the security and privacy of personal data held by platforms (discussed further in the "privacy and data protection" section of the previous paper in this series.)

One response is to limit the participants in an interoperability scheme to organisations that have contractually agreed to honour security and privacy requirements, and perhaps even be independently certified to do so. This is mandatory in the UK's Open Banking scheme, and has been proposed by Facebook in relation to data portability.[64] Similarly, the MyData scheme "intends to build trust in personal data services through a combination of transparency, interchangeability, public governance, respectable companies, public awareness, and secure technology".[65]

One data governance expert interviewee felt "Membership requirements have to be there, because of the sensitivity of the data both to individuals and to organisations, as part of the trust framework." An official interviewee commented: "if you don't know where your data are hosted, and you have three or four main actors, that's OK. You can find solutions if you have a finite set of actors. For messaging only, risks for privacy can be minor, it's really risks relating to content and especially cross-posting and to comment on content which can be riskier regarding all the data which are concerned, and which goes further than messaging." Another former official interviewee added: "there is a tension with GDPR as representing

[64] Facebook, Comment submitted to the US Federal Trade Commission 22 September public workshop "to examine the potential benefits and challenges to consumers and competition raised by data portability", 21 August 2020.

[65] Poikola, fn 34, p.7.

fundamental rights. It's not unreasonable for one participant to require compliance from others, unless it's pretextual."

However, several other interviewees disagreed with this notion. One SME developer commented: "while it could make sense that users have a way to learn where a contact's service operates from (i.e. if it's under the GDPR or not) and if it meets certain codes of conduct, I don't think that Facebook should be able to make that a requirement. It looks like an excuse to either not interoperate, or limit interoperability to a few big other players that could perhaps form a cartel with them. In any case, when I use my email service to send email to someone else that uses a different email provider, my email service doesn't require the recipient's service to be certified or to prove their practices. They just send my damn information where I want it to go, no questions asked. Why shouldn't social media work in the same way?"

One free software developer added:

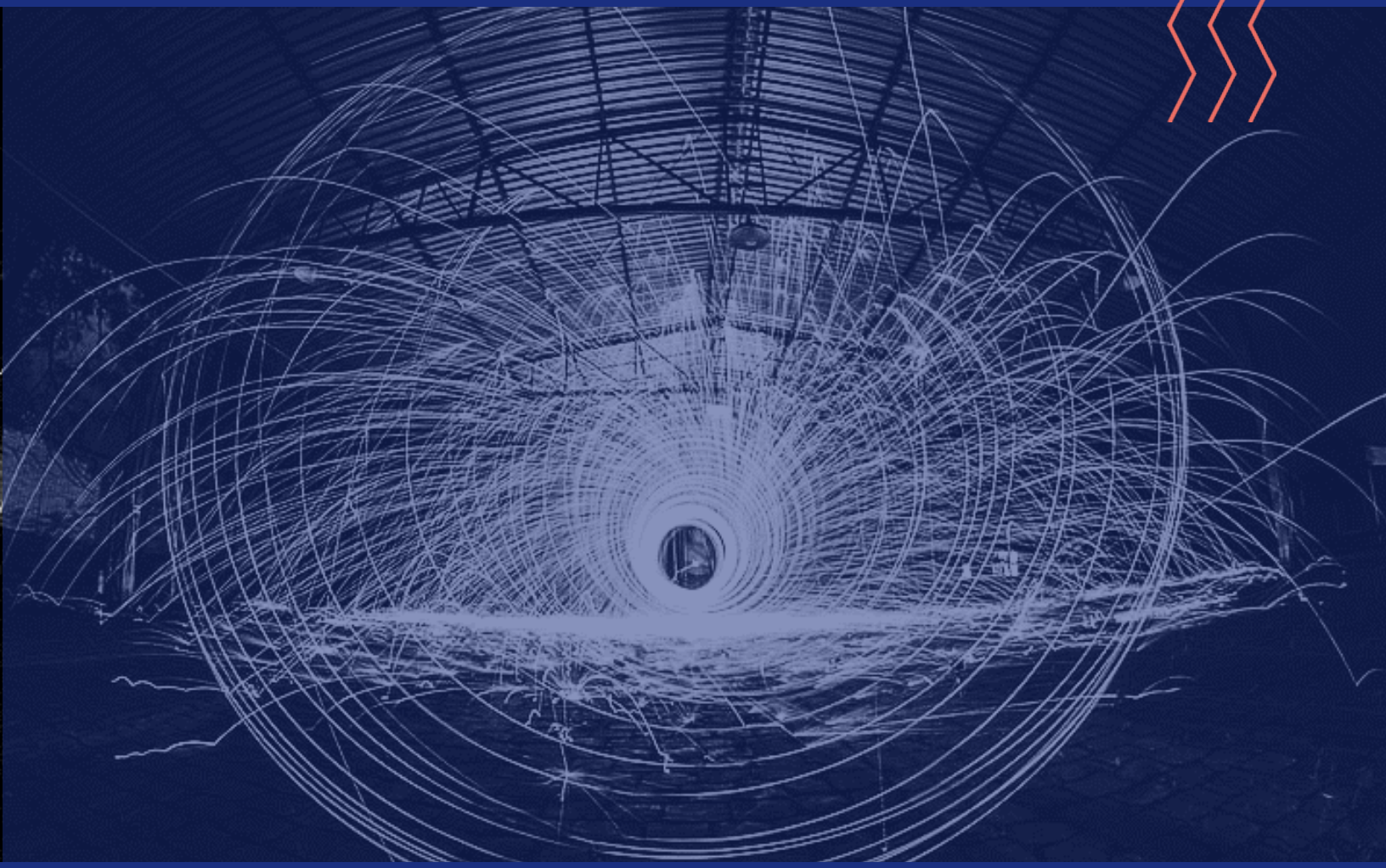
> *The ecosystem should be technically open, and you shouldn't need to have permission for your app (and an API key). I do not want to end up with apps being services. This is a big issue with API keys. Once as a developer you apply for an API key, you need to run your software as a service. It is a step forward if you as an individual user can write software to access the services you use. If you want a free software ecosystem you need this. That doesn't empower people. I should be able to fork someone's software, and not reapply, and the more complicated this system is the less likely people will do this. It's a step forward but it remains unfree. (I can well imagine we end up here. But it would be a compromise.)*
>
> *There may be a need for API keys as such, but a user should be able to get an API key. I should be able to use any software to log in to any service provider. That is a principle we need to keep emphasising. We need to separate the client and the server side. The server should be neutral to what client I use. That's what the US ACCESS Act calls delegation. We should put more focus on the software side of that.*

NOV 2020

The Technical Components of Interoperability as a Tool for Competition Regulation

Ian Brown

This paper is published with the OpenForum Academy, which is an independent programme established by OpenForum Europe. It has created a link with academia in order to provide new input and insight into the key issues which impact the openness of the IT market. Central to the operation of OpenForum Academy are the Fellows, each selected as individual contributors to the work of OFA.



ofa OpenForum Academy