Interoperability and the DMA in Action:

Developers Experiences of Data Portability API Access

Megan Kirkwood
interop.dma@gmail.com
11/11/2024

Table of Contents

Abstract 2
Introduction 3
Data portability before the DMA 3
Data portability and interoperability in the DMA 6
Literature review 8
Data portability 8
APIs 11
Standards 14
Methodology 16
Analysis 18
On RQ1) How easy is it for developers to access the APIs offered by the gatekeepers? 18
Google Data Portability API 19
Meta Portability Tools 24
LinkedIn Data Portability APIs 25
Amazon Data Portability API 26
TikTok P*ortability API* 27
Apple Account Data Transfer web API 27
On RQ2) Is there a need to create formal standards or open protocols? 29
Conclusion 34
References 35

Abstract

To evaluate the compliance of Digital Markets Act gatekeepers with Article 6(9) of the legislation, which mandates real-time and continuous data portability of end-users' data with authorised third parties, this article conducts a qualitative analysis of developer interviews. Interviews were conducted with developers seeking verification with gatekeepers' data portability tools, most of which were either introduced or improved in response to the law, to understand how the verification process works with each gatekeeper. This investigation included understanding how appeals work for access denial and whether excessive security barriers are in place. The second research question asked if there is a need to develop formal standards or protocols if gatekeepers' individual portability solutions were deemed inaccessible or if there is a need to redistribute power away from gatekeeper control and towards mutually agreed upon standards. The research found that verification for data portability is prohibitively difficult, with only Alphabet's Google Data Portability API being accessed by participants. However, Alphabet requires a security assessment which does not 'add much value' according to one participant, asks for redundant information, takes an excessive amount of time and costs money to complete. Participants accessed none of the other portability tools due to unclear verification processes and lack of correspondence. On the second research question, participants generally felt that technical standardisation is undesirable at this stage, but most argued that verification would be massively improved if carried out by an external independent body. The research concludes that further recommendations cannot be made until further assessment of the tools is carried out, particularly as some gatekeepers have announced planned improvements. That said, if verification remains prohibitively difficult, further feedback will be difficult to obtain, and the European Commission may have to engage with gatekeepers to improve verification for third parties.

Introduction

Data portability before the DMA

Data portability, meaning the ability of individuals to obtain and reuse their personal data for their own purposes across different services, has been a legal requirement since the General Data Protection Regulation (GDPR) became applicable in 2018.[1] Under Article 20 of the GDPR, individuals have the right to access personal data from a data controller and transport it to another data controller in a machine-readable format.[2] The European Data Protection Supervisor writes that this 'will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy'.[3] Thus, the benefit of data portability is that users

> can control the data by extracting it from a platform you no longer trust, and manage it directly, or offer it instead to a different service provider in whom you have greater trust. Competition thus emerges as the second purpose of data portability; regardless of your interest in data ownership or privacy values, if you can port your data to another service provider, you can switch services with low transactional cost.[4]

Therefore, the promise of data portability lies in increased control of personal data and the development of new competitors and industries, thus removing dependencies on large incumbent firms that dominate digital markets. For this to happen, first the incumbents must allow for portability. Despite various platforms creating tools for downloading data, for example, Meta's Download Your Information (DYI) tool[5] which pre-dates the GDPR and was initially launched in 2010, or Google's similar data download service Google Takeout[6] initially launched in 2011, such a flourishing of new services has largely not taken hold. Nicholas and Weinberg investigate why more services have not been successful despite the availability of portability tools, finding that ported Facebook data was largely useless for building competitor products, as many of the wider network interactions cannot be ported and the data was far too specific to Facebook to be of much use elsewhere.[7] There is also the

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/01

[2] Ibid.

[3] Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" (European Commission 2016) WP 242 rev.0 <https://ec.europa.eu/newsroom/article29/items/611233/en>, 4.

[4] Chris Riley, "Unpacking Interoperability in Competition" (2020) 5 Journal of Cyber Policy 94 <https://doi.org/10.1080/23738871.2020.1740754>, 96.

[5] Meta, "Download a Copy of Your Information on Facebook" (*Facebook Help Centre*, 2024) <https://www.facebook.com/help/212802592074644/>.

[6] Google, "How to Download Your Google Data" (*Google Account Help*, 2024) <https://support.google.com/accounts/answer/3024190?hl=en>.

[7] Gabriel Nicholas and Michael Weinberg, "Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?" (Engelberg Center on Innovation Law and Policy 2019) <https://www.law.nyu.edu/sites/default/files/Data%20Portability%20and%20Platform%20Competition%

simple fact that potential data endpoints are limited. When downloading data from Google Takeout, the destinations are either two Google-owned services or Dropbox and Box, which are both cloud storage providers. Meta fared slightly better, whose DYI service includes possible endpoints such as Google Photos, Dropbox, Backblaze B2, and Koofir cloud storage, as well as Photobucket, a paid-for service that enables the backup, sharing and embedding of photos and videos across devices and platforms.[8] Thus, the utility of data available through these tools and limited existing possible endpoints beyond merely cloud storage largely restrains users from proactively downloading their own information to give to third parties.

Going beyond data portability is interoperability. Whereas 'portability lets a customer take data about them from one firm to another [… i]nteroperability lets a customer use services from competing firms together'.[9] This requires the interoperable technologies to be compatible on a technical level which is 'widely acknowledged to prevent vendor lock-in (or dependency on a single company to provide a product or service) and stimulate innovation'.[10] Rather than users being locked into a dominant network, 'interoperability redefines the "property rights" on the network externalities as belonging to users, on both sides of the platform, and not the firm owning the dominant platform'.[11] This enables a fundamental shift in power towards users and away from dominant firms as users can easily switch between them but retain access to products, services or even social networks they want. Attempts encourage industry players to increase interoperability like the Data Transfer Initiative[12], a non-profit organisation, have seen some progress such as enabling the transfer of photos between Google and Apple's proprietary ecosystems.[13] However, progress has been slow, largely because the initiative relies on voluntary commitments which 'can also be seen as distractions to delay or avoid regulation'.[14] While more formal standard-setting bodies, like the World Wide Web Consortium (W3C) exist to create common standards which can increase interoperability, for example, HTML is a standard for displaying documents in a web browser, there are limitations as to their effectiveness. Beyond the slow process of creating standards, which are equally slow to change later, very real concerns exist in standard-setting power dynamics, as

---

20-%20Is%20User%20Data%20Exported%20From%20Facebook%20Actually%20Useful%20to%20Competitors.pdf>.

[8] "Photo Storage" (*Photobucket*) <https://photobucket.com/>.

[9] Ian Brown, "The UK's Midata and Open Banking Programmes: A Case Study in Data Portability and Interoperability Requirements" (2022) 2022 Technology and Regulation <https://techreg.org/article/view/11539>,114.

[10] Robert Bodle, "Regimes of Sharing: Open APIs, Interoperability, and Facebook" (2011) 14 Information Communication & Society 320 <https://doi.org/10.1080/1369118x.2010.542825>, 324.

[11] Fiona M Scott Morton and others, "Equitable Interoperability: The 'Supertool' of Digital Platform Governance" (2023) 40 Yale Journal on Regulation <https://www.yalejreg.com/print/equitable-interoperability-the-supertool-of-digital-platform-governance/>, 1019.

[12] Data Transfer Initiative, "Data Transfer Initiative Home Page" (*Data Transfer Initiative*, 2024) <https://dtinit.org/>.

[13] Chris Riley, "Data Transfer Initiative Members Apple and Google Introduce New Photo and Video Transfer Tool" (*Data Transfer Initiative*, July 10, 2024) <https://dtinit.org/blog/2024/07/10/DTI-members-new-photo-video-tool>.

[14] Chris Riley, "A Framework for Trusted, Safe Third-Party Data Transfers" (*Data Transfer Initiative*, November 7, 2023) <https://dtinit.org/blog/2023/11/07/framework-trust>.

> a powerful company could co-opt, under-mine or overrule the technical decisions being made in a standards process. The result could thus be built-in structural advantages for one company rather than uniform benefit and opportunity for all, yet all companies would be yoked to the deficit through the practical requirement to adhere to the dominant company's standard.[15]

Indeed, Doctorow points out that W3C is comprised of 'paid employees working on behalf of the largest tech companies'[16] so that adopted standards reflect their business interests. Doctorow points out that 'if the chair, co-chair and secretary all come from a single company (or a duopoly), that's fine, despite the fact that this means that the largest companies are literally setting the agenda'.[17] Allowing the current gatekeepers to set the agenda further increases their power as technologies are built around their business interests which may not be in the common interest.

Thus, the Digital Markets Act[18] (DMA) expands on the GDPR's data portability mandates by introducing increased legal obligations on the largest tech companies, including interoperability mandates. The DMA is a sector-specific regulation intended to complement competition law which entered into force on 1 November 2022 and became applicable on 2 May 2023. Companies providing 'core platform services', which include social networks, app stores, advertising networks, browsers, intermediation services, operating systems, video sharing, search, and messaging services, have to notify the Commission if they meet the quantitative thresholds specified in the legislation.[19] The Commission will then have 45 working days to adopt a decision designating a specific gatekeeper, which is a company operating one or more core platform services. The designated gatekeepers will have a maximum of six months after the Commission's designation decision to ensure compliance with the obligations and prohibitions in the DMA. As of 2024, there are seven gatekeepers with 24 core platform services between them. The gatekeeper firms are Alphabet, Apple, Amazon, Booking, ByteDance, Meta and Microsoft.[20] The seventh gatekeeper, Booking, was only designated on the 13th of May 2024, meaning it only came into compliance on the 14th of November; therefore, it is not included in this analysis.[21] Articles 5, 6, and 7 of the DMA comprise the various obligations imposed on gatekeepers regarding the operation of core platform services with the ultimate aim of removing barriers to entry for competitors and creating a fairer and more contestable digital marketplace.[22]

---

[15] Riley (n 4) 98.
[16] Cory Doctorow, *The Internet Con: How to Seize the Means of Computation* (Verso Books 2023), 77.
[17] Ibid, 79.
[18] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ 2 265/1
[19] Ibid, Article 3.
[20] European Commission, "DMA Designated Gatekeepers" (*Digital Markets Act (DMA)*, 2024) <https://digital-markets-act.ec.europa.eu/gatekeepers_en>.
[21] Booking – Online intermediation services (Case DMA. 100019) Commission Decision [2024] <https://ec.europa.eu/competition/digital_markets_act/cases/202442/DMA_100019_191.pdf>.
[22] Digital Markets Act (2022).

Data portability and interoperability in the DMA

Interoperability mandates within the DMA can be found in Articles 6 and 7.[23] Article 7 concerns the obligations of gatekeepers on interoperability of number-independent interpersonal communications services, or messaging services and apps, which concerns not only potential API use but also technical standards and debates about end-to-end encryption.[24] Article 6, on the other hand, covers a range of obligations and restrictions placed on the gatekeeper including obligations to provide data access to third parties.[25] Thus, to focus the research, the author focused on Article 6(9)[26] to investigate data portability technology and how it is evolving under the DMA. Under Article 6(9) when authorised by the end user, gatekeepers have to provide third parties with effective portability of data provided by the end-user or generated through the activity of the end user in the context of the use of the relevant core platform service.[27] Gatekeepers should provide free-of-charge tools to facilitate the effective exercise of such data portability, including the provision of continuous and real-time access to such data.

To effectively provide this level of continuous data portability, most gatekeepers will rely on the use of Application Programming Interfaces, or APIs. An API is 'an interface of a computer program that allows the software to "speak" with other software'.[28] APIs are important pieces of digital architecture, serving 'as the core infrastructural elements that underpin the large ecosystems of apps and services (or "complements") created by third parties and partners'.[29] Therefore, a great deal of this research will focus on the various APIs being offered by gatekeepers, which currently vary in terms of data access available, whether the data is real-time and continuous or ported in individual instances, and how easy it is to obtain access to the APIs. To measure the success of the DMA, close monitoring of gatekeepers' compliance with obligations will be necessary.

The gatekeepers currently offer the following data portability tools and APIs.

Alphabet	Amazon	Apple	ByteDance	Meta	Microsoft
'The Data Portability API lets you build applications that request	'Amazon Data Portability offers authorized third parties the capability to programmatically	'Use the Account Data Transfer web API to request and download	TikTok's Data Portability API 'makes it easier for users to	Download Your Information (DYI) is a tool to 'download a copy of information you've provided to	LinkedIn Pages Portability API is a 'program to enable Page owners, including Page admins and their

[23] Ibid.
[24] Ian Brown, "Private Messaging Interoperability in the EU Digital Markets Act" (2022) <https://openforumeurope.org/wp-content/uploads/2022/11/Ian_Brown_Private_Messaging_Interoperability_In_The_EU_DMA.pdf>.
Marc Bourreau, Jan Krämer and Miriam Buiten, "Interoperability in Digital Markets" (Centre on Regulation in Europe (CERRE) 2022) <https://cerre.eu/publications/interoperability-in-digital-markets/>.
[25] Digital Markets Act (2022).
[26] Ibid.
[27] Ibid.
[28] Stine Lomborg and Anja Bechmann, "Using APIs for Data Collection on Social Media" (2014) 30 The Information Society 256 <https://doi.org/10.1080/01972243.2014.915276>, 256.
[29] Fernando N Van Der Vlist and others, "API Governance: The Case of Facebook's Evolution" (2022) 8 Social Media + Society <https://doi.org/10.1177/20563051221086228>, 2.

authorization from a user to move a copy of data from Google services into your application'.[30]	import Amazon customers' data to an app or website after the customers give authorization through Login With Amazon (LWA)'.[31]	App Store information and app-install activity data on behalf of people who use your app'.[32]	transfer their data from TikTok directly to services and apps they authorize'.[33]	Facebook using the Download Your Information tool. You can download this information in an HTML format that is easy to view, or in a JSON format, which will allow you to transfer your information to another service'.[34] Meta's Transfer Your Information (TYI) tool 'makes it possible for people to transfer a copy of data such as photos, videos or posts to a variety of destinations such as Google Photos, Dropbox, and Koofr'.[35]	authorized third-party developers, to access their LinkedIn Pages data programmatically'.[36] Additionally, there is also a 'Member Data Portability (Member) product provides APIs that allow LinkedIn members to create an application to fetch that LinkedIn member's LinkedIn data'.[37]

To measure the success of Article 6(9), this research asks:

[30] Google for Developers, "Introduction: Develop Apps Using the Data Portability API" (*Google for Developers*, 2024) <https://developers.google.com/data-portability/user-guide/introduction>.
[31] Amazon, "Amazon Data Portability Overview" (*Amazon Developer*, 2024) <https://developer.amazon.com/docs/amazon-data-portability/overview.html>.
[32] Apple Inc., "Account Data Transfer" (*Apple Developer Documentation*, 2024) <https://developer.apple.com/documentation/AccountDataTransfer>.
[33] Sam Heft-Luthy, "Introducing TikTok's Data Portability API" (*TikTok for Developers*, 2024) <https://developers.tiktok.com/blog/2024-introducing-tiktok-data-portability-api>.
[34] Meta, "Accessing and Downloading Your Facebook Information" (*Facebook Contact Forms*, 2024) <https://www.facebook.com/help/contact/2032834846972583>.
[35] William Morland, "What's New with Data Portability and Our Transfer Your Information Tool" (*Meta*, October 22, 2022) <https://developers.facebook.com/blog/post/2022/10/18/data-portability-and-our-transfer-your-information-tool/>.
[36] LinkedIn, "LinkedIn Pages Data Portability API Application Review and Developer Support" (*LinkedIn Help*, 2024) <https://www.linkedin.com/help/linkedin/answer/a6216629>.
[37] Microsoft, "Member Data Portability (Member)" (*Microsoft Learn*, February 5, 2024) <https://learn.microsoft.com/en-us/linkedin/dma/member-data-portability/member-data-portability-member/?view=li-dma-data-portability-2024-08>.

RQ1) How easy is it for developers to access the APIs offered by the gatekeepers? This includes understanding access policies and how clear those policies are, the vetting process, and the process to appeal access denial. This aims to understand if there are potential unnecessary restrictions on third parties accessing APIs, as a major policy challenge in this area is understanding whether restrictions 'constitute a thoughtful response to a legitimate security concern, or an anticompetitive act designed to repress a competitor'.[38]

RQ2) Is there a need to create formal standards or open protocols? This seeks to address the differences between gatekeeper API offerings and whether those differences are beneficial to developers who may be able to adapt to different APIs or if there is a need to formalise a standard to increase overall interoperability.

Interoperability is at the heart of increasing contestability and fairness, the key driver of the DMA. This recognises that proprietary, siloed information ecosystems are often attributed as creating powerful lock-in effects where it is difficult to escape an ecosystem, resulting in 'competition *for* the market rather than *in* the market'.[39] Indeed, interoperability has been a key focus of the Commission's enforcement of the DMA thus far, particularly its scrutiny of Apple and forcing closed ecosystems to be pried open. For example, the Commission has launched its first specification proceedings to assist Apple in complying with its interoperability obligations under the DMA.[40] Therefore, this research aims to be a valuable contribution to understanding how the technical side of interoperability works so far, as monitoring API access is 'difficult, and yet critical for competition regulators'.[41] By answering the research questions above, this project aims to contribute to future DMA enforcement regarding data portability and whether further specification is needed for effective data portability and interoperability.

Literature review

Data portability

Data portability is enshrined as a right under the GDPR[42] yet, porting data is incredibly burdensome for individuals. Data downloaded through portability tools like DYI or Google Takeout are 'typically delivered as a bundle of technical files, hard to understand and often delivered without explanation'[43] which individuals do not know what to do with. Submitting 'portability requests [… can be] cumbersome to complete' and sometimes the data formats

[38] Riley (n 4) 98.
[39] Fiona Scott Morton and others, "Stigler Committee on Digital Platforms: Market Structure and Antitrust Subcommittee" (The University of Chicago Booth School of Business 2019) <https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report>, 29.
[40] European Commission, "Commission Starts First Proceedings to Specify Apple's Interoperability Obligations under the Digital Markets Act" (*Digital Markets Act (DMA)*, September 19, 2024) <https://digital-markets-act.ec.europa.eu/commission-starts-first-proceedings-specify-apples-interoperability-obligations-under-digital-2024-09-19_en>.
[41] Riley (n 4) 100.
[42] General Data Protection Regulation (2016) Article 20.
[43] Alex Bowyer and others, "Human-GDPR Interaction: Practical Experiences of Accessing Personal Data" (2022) 106 CHI Conference on Human Factors in Computing Systems 1 <https://doi.org/10.1145/3491102.3501947>, 10.

are not machine-readable, in violation of the GDPR.[44] Beyond being difficult for the average user, there is a 'lack of value that individuals can create when porting their data. The value increases, however, if the individual can transmit this data to another service'.[45] Therefore, examining the current limitations of portability tools may provide answers as to how to improve them, which increases the overall value and utility of porting data.

It is generally accepted that data '[p]ortability should also facilitate innovation because the recipient of useful data can create new products and services; this would create new competition and even new markets'.[46] However, the value of the data being ported could be a barrier. Toropainen argues that because 'Article 20 of the GDPR is limited, among other things, to personal data "provided by" the data subject' individuals 'self-determination' is limited because 'they cannot control data created through their actions' which limits the usefulness of the data.[47] DMA Article 6(9) aims to solve this by including data generated by a user's activity. While this increases the potential value of the ported data, it equally highlights the tension between competition and data privacy. Though more data being ported may be more valuable to the receiving party and helps reduce switching costs for end users, the more data that is ported the bigger the privacy concern, as articulated by Nicholas and Weinberg

> When one of those users decides to export her data, a platform must define the frontiers of where her data ends and another user's begins. […] A data portability program designed to maximize competition would allow users to export data that includes entire comment threads (not merely the user's contribution), the identities of their friends, and data uploaded by others that relates to the exporting user (for example, a photo of the exporting user's face, taken by someone else). This would make it easier for the exporting user to replicate her experience and reconstruct her social network on a new platform.[48]

However, this not only eradicates the consent of users whose data would also be exported along with the primary exporter, but it also illustrates the excessive nature of data collection practices by incumbents and transports that logic onward. This example illustrates 'how competition law's data democratization policies can clash with privacy law's data minimization policies'.[49] Stucke argues that policymakers should not rely 'too heavily on data-openness policies', as this 'will promote an economy where we become the commodity—where the ensuing toxic competition is how to extract even more data about us (but not for us) and increase our addiction to their websites and apps'.[50] This is not to suggest abandoning data portability altogether, which Stucke recognises is essential to create meaningful innovations, as well as recognising that data hoarding by incumbents is bad for both privacy and power concentration. Her conclusion is to promote an economy no longer based on behavioural advertising, which creates a race to the bottom for extractive data

---

[44] Sanna Toropainen, "The Right to Data Portability in the Fair Data Economy" (Sitra 2023) <https://www.sitra.fi/en/publications/the-right-to-data-portability-in-the-fair-data-economy/>,.23.
[45] Ibid, 24.
[46] Morton and others (n 11) 1027.
[47] Toropainen (n 44) 30.
[48] Nicholas and Weinberg (n 7) 3.
[49] Maurice E Stucke, "The Relationship between Privacy and Antitrust" [2022] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4042262>, 412.
[50] Ibid, 414.

hoarding. Instead, she suggests facilitating applications and services that 'harness the value from data to promote an inclusive economy, that protects our autonomy, well-being, and democracy'.[51] This is a similar conclusion to Nicholas and Weinberg, who argue that 'there may be reason for concern about the kind of innovation Facebook data might encourage. To the extent that exported data might be useful for building a new platform, that platform is mostly likely to be based on invasive, highly targeted advertising'.[52] That said, they see value in data portability that 'facilitate[s] the concept of data ownership—a value that may have importance independent of competitive concerns'.[53] Therefore, on the one hand, increased portability helps remove data power from incumbents' hands. Still, on the other hand, there must be an acknowledgement that strong data protection must be upheld and consideration of the current economic incentives for data collection.

Fenwick, Jurcys and Minssen, point out the second reason that data portability has largely been useless. Under Article 20 'data controllers are generally not required to adopt or maintain data processing and transfer systems that are technically compatible with other controllers in different organisations'.[54] This means previously, data downloads were done in single instances which meant data could not be kept up to date easily and could not be merged with data from other firms due to differences in format. This decreased the value of data and made it cumbersome for the user who has to manually download the required data and then port it. Again, this is addressed in the DMA as data portability must be real-time and continuous under 6(9). However, what real-time and continuous means seems to be up for debate. For example, Amazon's Data Portability API allows for daily downloads of customer data generated on or given to the Amazon Store and Ads for authorised third parties.[55] Apple allows users to download data daily, as does Microsoft's LinkedIn Members API.[56] Similarly, Meta's DYI and TYI tools have introduced the option of daily data transfers, with Meta representatives stating explicitly that 'daily is real-time'.[57] Google's Data Portability API only allows for single transfers with the user needing to reverify transfers, though this is currently being amended.[58] ByteDance representatives said there are no limits on requests for data that developers can make through the TikTok Data Portability API beyond some 'thousands per minute'.[59] This illustrates Morton and others' argument

---

[51] Ibid, 416.
[52] Nicholas and Weinberg (n 7) 2.
[53] Ibid, 3.
[54] Mark Fenwick, Paul Jurcys and Timo Minssen, "Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow" [2024] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4475106>, 9.
[55] European Commission, "Compliance with the DMA: Amazon" <https://webcast.ec.europa.eu/compliance-with-the-dma-amazon-2024-03-20>.
[56] Apple Inc., "Apple's Non-Confidential Summary of DMA Compliance Report" (European Commission 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>, p. 10.
Microsoft, "Non-Confidential Version 1 Microsoft Compliance Report – Annex 11 – LinkedIn (Online Social Networking Service)" (European Commission 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>, 136.
[57] European Commission, "Compliance with the DMA: Meta" <https://webcast.ec.europa.eu/compliance-with-the-dma-meta-2024-03-19>.
[58] Google for Developers, "Data Portability API Release Notes" (*Data Portability API*, 2024) <https://developers.google.com/data-portability/docs/release-notes>.
[59] European Commission, "Compliance with the DMA: Bytedance" <https://webcast.ec.europa.eu/compliance-with-the-dma-bytedance-2024-03-22>.

> that self-regulation will not work in this setting. It may be tempting to allow the dominant firm to design the APIs and simply publish them for everyone else to use. But if the dominant firm is placed in charge, it has the incentive and ability to alter the interface every time a threatening competitor appears likely to obtain any significant market share.[60]

Limiting the API call limits is but one example of how incumbents' control of portability tools should be examined closely to ensure that they are not merely further entrenching their market position and power.

APIs

Though the history of API development dates back to 1948,[61] the first use of the term API appeared in 1968 in discussing hardware-independent application program interfaces.[62] APIs became popular software modules in the 2000s with the popularisation of the Internet and the creation and growth of online businesses through web APIs, which are 'software modules that encapsulate resources (e.g., data, storage, or computing resource), which are accessible via the Internet'.[63] Evans and Basole write that open-access web APIs had a thirtyfold increase from 2006 to 2016, noting that the API economy was dominated by digital companies, naming Google, Microsoft, Facebook, Amazon, eBay, Yahoo, Salesforce and Twilio.[64] This increase in API usage coincides with the rise of digital platforms, which initially relied on third parties, including end users, to contribute to the platform itself. In computer science terms, platforms are a 'set of digital resources— including services and content—that enable value-creating interactions between external producers and consumers'.[65] The emphasis on 'value-creating interactions' makes clear that '"platforms" are "platforms" not necessarily because they allow code to be written or run, but because they afford an opportunity to communicate, interact or sell'.[66] Platforms are not entirely separate from each other; they are dynamic and interactive. Helmond notes that the platformisation of the Internet is a progression from changes in Web culture and infrastructure.[67] Whereas the early Web was

---

[60] Morton and others (n 11) 1032.

[61] Herman Goldstine and John Von Neumann, "Planning and Coding of Problems for an Electronic Computing Instrument: Report on the Mathematical and Logical Aspects of an Electronic Computing Instrument Part II Vol III" (Princeton University Institute for Advanced Study 1948).
- discusses coding subroutines which led to API creation.
Joshua Bloch, "A Brief, Opinionated History of the API" (New York, United States of America) <https://www.infoq.com/presentations/history-api/>.

[62] Ira W Cotton and Frank S Greatorex, "Data Structures and Techniques for Remote Computer Graphics" [1968] Association for Computing Machinery <https://doi.org/10.1145/1476589.1476661>.

[63] Neng Zhang and others, "Web APIs: Features, Issues, and Expectations – A Large-Scale Empirical Study of Web APIs from Two Publicly Accessible Registries Using Stack Overflow and a User Survey" (2022) 49 IEEE Transactions on Software Engineering 498 <https://doi.org/10.1109/tse.2022.3154769>, 498.

[64] Peter C Evans and Rahul C Basole, "Revealing the API Ecosystem and Enterprise Strategy via Visual Analytics" (2016) 59 Communications of the ACM 26 <https://doi.org/10.1145/2856447>.

[65] Terry Flew, "The Platformized Internet: Issues for Internet Law and Policy" [2019] Journal of Internet Law <https://eprints.qut.edu.au/129830/>, 4.

[66] Tarleton Gillespie, "The Politics of 'Platforms'" (2010) 12 New Media & Society 347 <https://doi.org/10.1177/1461444809342738>, 351.

[67] Anne Helmond, "The Platformization of the Web: Making Web Data Platform Ready" (2015) 1 Social Media + Society 205630511560308 <https://doi.org/10.1177/2056305115603080>.

merely static, Web 2.0 is far more participatory, and platforms became a means for this participation.[68]

APIs are important in facilitating this participation. Lomborg and Bechmann write that APIs enable the 'development and enhancement of the core social media services' by third-party developers.[69] Thus, APIs for platform development were initially encouraged.[70] Platforms became a central point of interaction with users of the web, with platform incumbents increasing in popularity. Network effects, meaning 'when the benefit of network participation to a user depends on the number of other network users with whom they can interact' helped to grow the market dominance of incumbents, leading to 'winner takes all' marketplaces.[71] This also explains why the API economy is dominated by Google and Facebook[72] as developers seek to make applications compatible with these popular services and business partners seek to reach those audiences.[73] Ideally, this is an equally beneficial relationship where third parties can take advantage of the incumbent platform's audience reach and data pools, whilst contributing value back to the platform in the form of complementary apps. However, the benefits largely bend in favour of incumbents and can leave complementary services dependent on those connections. To take one example, in the 2010s,

> Facebook appealed to third-party app developers to implement its social buttons on their websites and released the Open Graph protocol (2010) to standardize data formats on the web. This was a strategic move that helped make a wealth of external (i.e., unstructured) data sources "platform ready" to integrate them into Facebook's data infrastructure.[74]

The expansion of Facebook across the web, via like and share buttons or using Facebook Login to access third-party websites and services has had 'the effect of consolidating an API's provider services over time (as seen in the present precedence given to privately controlled login services over earlier non-profit and open standard efforts such as OpenID)'.[75] Developers were encouraged to make certain uses of data, such as rich social apps to keep

---

[68] Ibid.

[69] Lomborg and Bechmann (n 28) 256.

[70] For example, a third-party application called Tweetie, originally released in 2008, was an application made for iOS and Mac devices to access Twitter (now X), which at that time did not have a mobile or desktop application but only ran on web browsers. The Tweetie application even developed the pull-to-refresh function so well-known to Twitter users. Twitter acquired Tweetie in 2010 to become the official iOS application.
Nilay Patel, "Twitter Granted Patent on Pull-to-Refresh, Promises to Only Use It Defensively" *The Verge* (May 21, 2013) <https://www.theverge.com/2013/5/21/4350826/twitter-pull-to-refresh-patent-innovators-patent-agreement-announced>.

[71] David P McIntyre and Arati Srinivasan, "Networks, Platforms, and Strategy: Emerging Views and Next Steps" (2016) 38 Strategic Management Journal 141 <https://doi.org/10.1002/smj.2596>, 143.
Flew (n 65) 4.

[72] Evans and Basole (n 64).

[73] Fernando N Van Der Vlist and Anne Helmond, "How Partners Mediate Platform Power: Mapping Business and Data Partnerships in the Social Media Ecosystem" (2021) 8 Big Data & Society 205395172110250 <https://doi.org/10.1177/20539517211025061>.

[74] Fernando N Van Der Vlist and others (n 29) 11.

[75] Eric Snodgrass and Winnie Soon, "API Practices and Paradigms: Exploring the Protocological Parameters of APIs as Key Facilitators of Sociotechnical Forms of Exchange" [2019] First Monday <https://doi.org/10.5210/fm.v24i2.9553>.

users on the platform, and discouraged from creating applications such as data exporting.[76] As developers and businesses increasingly cater to large platforms, those platforms maintain power and control over what can be developed. This puts developers at the mercy of API changes or discontinuations, as

> Any change may cause disturbances or ripple effects across the entire ecosystem of apps and services relying on an API, potentially impacting the viability of all apps and services supported or sustained by it, including those of businesses and academic researchers. When Facebook changed API access to friends' data in 2014–2015, this severely impacted the business models and apps of complementors as well as academic research tools, causing shutdowns across the ecosystem.[77]

Thus, APIs may not only represent information asymmetries, meaning developers and business partners seek to access the vast audience and data pools of platforms, but power asymmetries as well. While 'third-party developers often bring a platform's service into a more imaginative and engaging light, and in doing so often enhance the ecology of a platform's success' any openness that was initially encouraged 'often tends to eventually be shut down once a platform has achieved relative dominance'.[78]

Where once API development was encouraged, it is generally accepted that following the Facebook-Cambridge Analytica scandal of 2018[79], many platforms closed off general access to APIs.[80] In most cases, this was done under the guise of security and privacy, although wealthy commercial institutes still could access platform data through their vast 'resources to buy data from commercial social media data resellers, or the wherewithal to engage in data acquisition through large-scale scraping or other unauthorised means'.[81] Bruns points out that Facebook 'deliberately sought to obscure the fact that the platform's fundamental business model had ostensibly enabled the emergence of Cambridge Analytica and similar political and advertising microtargeting services'.[82] This illustrates that data collection and use for ad targeting has not ceased due to the Cambridge Analytica scandal, however, encouragement of API use and service development dropped dramatically, with Facebook 'reportedly suspend[ing] some 200 third-party apps'.[83] API access changes were often issued without prior warning to those dependent on those APIs. API access has since been a contentious issue, as large platforms are able to cut off access to APIs under the guise of security and privacy, with little oversight into whether those are legitimate concerns or anti-competitive ones.[84] There are indeed a number of legitimate privacy and security

---

[76] Van Der Vlist FN and others (n 29).
[77] Ibid, 17.
[78] Snodgrass and Soon (n 75).
[79] Emma Graham-Harrison and Carole Cadwalladr, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach" *The Guardian* (March 17, 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
[80] Axel Bruns, "After the 'APIcalypse': Social Media Platforms and Their Fight against Critical Scholarly Research" (2019) 22 Information Communication & Society 1544 <https://doi.org/10.1080/1369118x.2019.1637447>.
[81] Ibid, 1550.
[82] Ibid, 1548.
[83] Ibid.
[84] Doctorow (n 16) and Riley (n 4).

concerns associated with APIs[85], and it is the responsibility of the API controller to ensure that APIs adhere to tight security measures to protect users from having their information taken by malicious actors. However, Morton and others suggest that regulators should 'not reject interoperability because privacy cannot be made perfect, but rather design interoperability so that privacy is not degraded relative to the setting without interoperability'.[86]

Standards

Standards, or standard protocols

> are sets of instructions in code that enable interoperability and data portability retroactively and prospectively, ensuring compatibility with all other platforms adopting the same standard. Unlike provider-specific solutions, they are developed in a technology-neutral manner by open, industry, or government standards bodies.[87]

Standards are useful as they provide uniformity, for example, plugs are a standard that enables a variety of products to be made that can rely on the standard for electricity supply resulting in large numbers of consumers being able to use it. Digital standard protocols equally enable uniformity and network connectivity, such as HTTPS for reading browser documents or OAuth, an industry-standard protocol for authorisation.[88] Most of the gatekeepers use OAuth within their verification process for portability API access, as will be explored in the analysis. Standards are usually created through open dialogue between industry members and governments can ask for standards to be developed for public use. Under the DMA, the Commission may request the European standards bodies to develop technical standards. Recital (96) states that gatekeeper obligations, particularly those related to data access, data portability or interoperability could be facilitated by the use of technical standards and the Commission can request European standardisation bodies to develop them.[89] This is further iterated under Article 48 which again gives the Commission the power to order the development of appropriate standards.[90]

Brown's research suggests that because APIs are endpoint interfaces often designed by one party for the use of others, the dominant party creating the API sets all the terms and that open protocols may be a preferable alternative.[91] Brown points out that standards can have a power-shifting effect as they allow

---

[85] McKinley Sconiers-Hasan, "Application Programming Interface (API) Vulnerabilities and Risks" (Carnegie Mellon University 2024) <https://insights.sei.cmu.edu/library/application-programming-interface-api-vulnerabilities-and-risks/>.
[86] Morton and others (n 11) 1035.
[87] Chinmayi Sharma, "The Present and Future of Data Portability: A Collected Volume of Independent Scholarly Research" (The Data Transfer Initiative ed, The Data Transfer Initiative 2024) <https://dtinit.org/assets/DTI-Data-Portability-Compendium.pdf>, 42.
[88] "OAuth Community Site" <https://oauth.net/>.
[89] The Digital Markets Act (2022).
[90] Ibid.
[91] Ian Brown, "The Technical Components of Interoperability as a Tool for Competition Regulation" (OpenForum Academy 2020) <https://www.openforumeurope.org/wp-

> 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 players are not interested in [standards], because you're basically trying to displace them".[92]

Standards are usually voluntary; therefore, they rely on the biggest players to adopt them to make them useful, otherwise, developers will cater their apps and services to work with incumbent firms rather than standards. This threatens the benefit of adopting standards which is supposed to level the playing field. If the Commission were to mandate the creation and adoption of protocols to enable portability under the DMA, a European standards-setting body such as the European Telecommunications Standards Institute (ETSI) would be responsible. ETSI is a non-profit organisation independent of government but has been recognised as an official European Standards Organisation. Brown interviewed several standards body experts with one interviewee commenting that

> 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.[93]

Doctorow equally describes how 'standards organizations are generally optimized *for* corporate capture' despite being structured as non-profits.[94] While standards bodies are comprised of civil society, academia, non-profits and small organisations, they are largely dominated by industry. This is not inherently negative as the point of standards bodies is to create technical protocols to be adopted by industry and requires industry expertise. Though theoretically 'participation is often formally open to commercial and non-commercial actors alike, […] in practice, industry representation outweighs public interest representation'.[95] Doctorow explains that civil society representation often relies on part-time employees or volunteers, while industry, particularly the largest firms, can employ swathes of full-time staff to work on standards development and represent the company in standards organisations.[96] ETSI membership contributions are calculated by classification derived from the member company's annual ECRT (Electronics Communications Related Turnover). Each classification corresponds to an annual contribution fee payable and a related voting weight, with small companies having smaller voting weights and higher classes gaining a higher voting weight.[97] Therefore, it is easy to see how the biggest companies can easily sway the output of standards organisations due to having more resources and more voting power.

That said, there are positive examples of legally mandated standards development lowering the barrier to entry and facilitating widespread innovation. The UK's Competition and Markets Authority (CMA) required large banks to cooperate in creating and

---

content/uploads/2020/11/Ian_Brown_The_technical_components_of_interoperability_as_a_tool_for_competition_regulation.pdf>.

[92] Ibid, 11-12.

[93] Ibid, 13.

[94] Doctorow (n 16) 77.

[95] Ayelet Berman, "Industry, Regulatory Capture and Transnational Standard Setting" (2017) 111 AJIL Unbound 112 <https://doi.org/10.1017/aju.2017.29>, 114.

[96] Doctorow (n 16).

[97] ETSI, "What Does Membership Cost?" (*ETSI*) <https://www.etsi.org/membership/dues>.

implementing technical standards for Open Banking as a way to address market concentration in banking. The biggest banks were required to agree upon an 'open API standard, data format standards, security standards, governance arrangements, and customer redress mechanisms'.[98] Brown states that 'the Open Banking programme has attracted a significant number of users and participating firms, with over 4 million personal and small business customers, and over 750 firms supplying compatible products and services by February 2021'.[99] The success of the initiative relied on mandating the biggest banks to participate, as an earlier self-regulatory initiative failed due to lack of uptake. The programme worked when an agreed upon single set of standards was adopted, as this 'made it much easier for competitor firms to use them, rather than having to deal with different technical standards for each of the nine regulated banks'.[100] This example of generally successful standards implementation could be leveraged in implementing some of the technical DMA mandates, as forcing the gatekeepers to create a single set of standards could make it easier for third parties to interoperate with them, facilitating fairness and contestability.

However, it should be noted that creating standards is slow due to all involved parties needing to reach a consensus based on the best technology available and overcoming potential competing interests. The downside to standards is that they are difficult to change once set, and 'could lock in market participants to a subpar standard, especially if the standard has been built under the influence of incumbents'.[101] Sharma writes that it is too soon 'to mandate specific technological implementations' as the current 'data is insufficient to conclusively favor standard protocols, webhooks, or any other method as the best means of achieving interoperability and data portability in a specific context. There is a dearth of research in the space'.[102] However, they state that once 'there is a clear understanding of the most effective practices' the Commission could encourage the development and adoption of 'nascent standards implementing these technical solutions' so long as it meets the goals of the DMA.[103] Therefore, while it is certainly too early to suggest mandating standards at this stage, it is a potential solution to consider in the future if gatekeeper APIs and portability tools are overly cumbersome or unusable for developers.

Methodology

This study is designed to seek the perspective of developers attempting to build products and services utilising the data portability opportunity offered by the DMA. Therefore, the author conducted a qualitative analysis through semi-structured interviews with seven developers, mostly business owners in various stages of app development and deployment. The interviews were conducted between September 2024 and November 2024. Interviewees were chosen purposefully, based on their occupation and interest in data portability, and represented select, information-rich cases. It is important to note that the gatekeepers did not release information regarding their data portability tools before the March 7th, 2024,

[98] Brown (n 9)117.
[99] Ibid, 122.
[100] Ibid,123.
[101] Ibid, 121.
[102] Sharma (n 87) 48.
[103] Ibid, 50.

compliance deadline.[104] Therefore, developers could not prepare applications for access in advance of the deadline meaning that it is too early for widespread uptake. Consequently, it was deemed more useful to conduct interviews with a small group rather than other quantitative methods such as large sample surveys. The research questions drove the formulation of the questionnaire, which was additionally aided by two preliminary interviews.

Questions asked to interviewees:

1. Tell me about the product that you are developing. What is it and what interoperability problem is it trying to solve?
2. Did the DMA inspire you to create this product or were you already developing before becoming aware of the law?
3. Have specific DMA mandates helped to realise your product? For example, Article 6(9)
4. What has your experience been with obtaining access to portability tools (if you have accessed any)? Was it easy/difficult? Do you receive ongoing support or correspondence?
5. Do you think that data sharing from the user's point of view is easy? Do you have suggestions for improvement?
6. Is there a need to develop interoperability standards more formally?
7. Is there anything that I should have asked but didn't?

The first question was chosen to introduce the interviewee and understand its business case for porting data from gatekeepers and what use that data might have. The second and third questions were chosen to understand what impact the DMA is having on businesses and to understand if 6(9) and data portability are useful for those businesses. Question four aims to get specific feedback on any APIs accessed, to understand the verification process and, if applicable, what the appeal process is like. The aim of this is to understand if gatekeepers are making API access difficult unnecessarily, perhaps in violation of the DMA or not respecting users' right to port their data under the GDPR, or if their security measures are reasonable in light of the potentially sensitive data that is being ported. While question five tended to be addressed when answering question two, this question was formed after a preliminary interviewee pointed out that if portability is not easy on the user side it is unlikely to be adopted. This issue has a history considering the lack of portability uptake under GDPR, thus, evaluating user consent flow under the new portability tools is of high importance. Question six addresses the potential future need to mandate standards and addresses the differences between each gatekeeper's data portability approach. The final question was asked in order to catch any important points that had been missed in the discussion, recognising the interviewee's technical expertise and experience.

After transcribing interviews, the author coded the interviews and conducted an inductive thematic analysis to compare interviewee answers based on themes identified. This

[104] European Commission, "Compliance Reports" (*Digital Markets Act (DMA)*, 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>.

helped to spot the similarities and differences between answers, for example, coding themes like API verification, authorisation, discussions on standards etc made for easier comparison between answers. The interviewees signed consent forms acknowledging their answers would be used for this study, under the condition of anonymity. Therefore, in the analysis, the names of participants and their businesses, including any identifying characteristics, have been removed. Interviewees have been named Research Participant (RP) 1-7. It should be noted that only five of the seven interviewees attained access to data portability APIs, with the other two participants deemed to be experts on data portability and have experience with other gatekeeper APIs and technical expertise. Their input is particularly important in answering RQ2.

Analysis

On RQ1) How easy is it for developers to access the APIs offered by the gatekeepers?

This includes understanding access policies and how clear those policies are, the vetting process, and the process to appeal access denial.

APIs are seen by most research participants as the most suitable tool for data portability, with RP1 stating that it is the safest and most secure tool as well as the most widely adopted. Participants reported that, because APIs are able to handle the facilitation of data sharing automatically, the consent flow on the user side is much easier compared to previously when users had to download a copy of their data and manually upload it to third parties. RP1 states that

> the initial flow for the user, for the portability aspect of it, is really simple and easy, comparatively speaking. They're not installing a separate piece of software, they're not waiting around, they're not having to upload it themselves. It's just via an API in the back end. Then you've got a fighting chance, I think, to be able to do this. That flow from our end now looks really, really easy.

RP6 also said that the user side of the consent flow has been significantly improved ‘if you compare it to what we've had before, it's [now] unbelievably easy. It's gone from being impossible to actually there is a thing’, adding that ‘the 6(9) element of the DMA is the crux of our business model’. Similarly, RP2 found that directly thanks to the DMA, their company was able to obtain data that was previously unobtainable and is much more ‘simple and intuitive’ for users to grant access to, rather than having to download and transfer a copy. RP4 has previously worked on a research project to develop and encourage a national identity verification tool, finding that the

> biggest problem is how to get people to enter their data? Therefore, and that remains the case, the DMA tackles one of your top three problems. If you can figure out how

> to make that population of data stored for a person easier and more useful because the DMA exists, well, yes, it's massive. Because it gives you the scale.

Therefore, the promise of 6(9) has the potential to open up new businesses and give the wider population, rather than those with already existing technical knowledge, control over their own data. The following section will look at the different portability tools offered by DMA gatekeepers.

Google Data Portability API

Google's Data Portability API scores the highest in terms of developer accessibility. Except for two research participants who did not want to connect to the API, all interviewees had either been verified or were in the process of being verified. RP2 cited that the pre-verification access to the Google Data Portability API meant that their team could use real data to help build their product. Pre-verification access to the API is allowed either for 'personal use' apps capped to 100 users who must approve access, known as whitelisting, to the third party, or apps in development/testing/staging.[105] Personal use or apps still in development do not require verification and only need to be verified through the OAuth protocol and to have a developer account.[106] RP4 also applauded the ease of access to the Google Data Portability API, as they were testing the API posing as a developer trying to integrate them into an app still in development, meaning it was eligible to bypass verification. Allowing easy access to APIs for small apps and apps in development was seen as a positive by participants and could be considered by other gatekeepers as a way to strengthen their API accessibility.

However, when it came to businesses seeking to scale and launch, verification was required for API access. RP1, 2, and 6 reported that the process of verification has taken a long time. RP1, at the time of the interview, still had not been verified after a month and a half, RP2 completed the verification process in seven weeks and RP6 reported that the process took three months. These participants reported that it was not necessarily that Google demanded excessive information but that the verification process was lengthy, with long waiting times between correspondences. RP2 said of the process that

> there are always minor things that you have to change. Just for that minor thing, you have to wait maybe two weeks because they take two weeks to respond. So, it is just a really slow process, and it seems like it's made on purpose. It's not that it's something that requires you to work on that for two weeks, and therefore it takes two weeks. No, it takes you five minutes, but then you have these minor changes based on their feedback that comes once in a while and therefore it ends up being a really long process.

RP6 similarly described that they

> would go quite long periods without hearing anything from Google. Then out of the blue, we'd get a request to answer a pretty trivial question. Then we'd have another

---

[105] Google, "When Is Verification Not Needed" (*Google Cloud Platform Console Help*, 2024) <https://support.google.com/cloud/answer/13464323>.
[106] Ibid.

> long wait, and then we'd get asked to add a sentence to our privacy policy. And then another long wait.

RP1 also described the process as slow and cautious, describing the tension between their company and Google, stating that they were stuck in a back-and-forth about user interface (UI) design, as RP1 wanted to tell the user that their data would be used to personalise their product

> from our perspective, we want to sell the feature. From their perspective, they want to say, "you're using Google to port your data. This is what it's got to say." It's very restrictive. They still hold all the power over that verification process. It could go on for months. We don't know. They still hold all the cards on that basis.

This appears partially due to regulatory uncertainty and discrepancy in data ownership perception. Google appears to understand that the data they hold belongs to them, rather than understanding the data belongs to the user, as is enshrined in the GDPR which states that portability is a right. RP3 eloquently describes that

> if the user gives consent, that's because the data belongs to the user. They are stored on a company server. They're used by the company. They're exchanged by the company. They're deleted maybe even by the company. But it still remains associated with the user who owns the rights of use of that data. That is particularly relevant and important with data portability and with what type of APIs are going to be available in the market as to who's going to have the right to use the data once the data has been ported. At the moment, the industry is completely stuck.

This is a long-standing issue, as Bernal notes regarding data sharing '[d]ue to the presence of privacy regulations, when personal data enter the equation, companies adopt a more stringent and hierarchical control mechanism'.[107] Understandably, as data controllers under the GDPR, Alphabet and other gatekeepers are responsible for ensuring that data can only be shared by authorised parties and that personal data is secure.[108] However, they are equally responsible for ensuring data subjects can exercise their rights, such as data portability.[109]

RP2, 5 and 6 were further along the verification process at the time of their interviews and added that Alphabet requires additional security verification with an external firm, TAC Security.[110] According to Google, apps that request access to Google users' restricted data and have access to data from or through a third-party server must go through a security assessment from TAC Security, completing the tier two cloud application security assessment framework (CASA). Google says the assessment 'helps keep Google users' data safe by verifying that all apps that access Google user data demonstrate the capability to handle data securely and to delete user data upon a user's request'.[111] Apps are required to be reverified every 12 months and if Google deems an app update to be a major update, the app may need

---

[107] Jaime Bernal, "Private Sector Trust in Data Sharing: Enablers in the European Union" (2024) 6 Data & Policy <https://doi.org/10.1017/dap.2024.20>, 4.
[108] General Data Protection Regulation (2016), Article 5(1 f).
[109] Article 29 Data Protection Working Party (n 3).
[110] TAC Security, "TAC Security" (2024) <https://tacsecurity.com/>.
[111] Google for Developers, "Restricted Scope Verification" (*Google Identity*, July 16, 2024) <https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification?hl=en>.

to undergo re-verification. Google chose this security assessment to standardise the process which is based on the OWASP Application Security Verification Standard (ASVS).[112] This standard aims to provide 'a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development'.[113] In theory, implementing a standardised security assessment should enable transparency regarding what is required to pass verification, and essentially enable a developer to be eligible to pass security assessments of any firm implementing the standard which could make API verification smoother. However, to pass the CASA tier two check, developers must either undergo a lab test by TAC or complete a self-assessment by scanning their application utilising 'CASA recommended scanning tools' and upload the result to the App Defence Alliance for validation.[114] The lab test has different costing options according to RP5, who explained that

> the lowest tier was $250 for a one-time verification. So, if within one application, you don't pass the test, you have to pay again. And so, we went with the second option, which was $750 if I remember correctly. This option guarantees that until you pass the verification, you can submit applications.

RP2, 5 and 6 all went with the lab assessment option. Looking at publicly accessible online forums, developers who opted for self-assessment said that the assessment took an excessive amount of time and that Google's instructions were very unclear meaning they had to look outward for direction and advice. This means it is likely that most developers would opt for the lab test option.

Research participants who reached the stage of undergoing the CASA assessment via TAC had generally negative experiences of the process. RP2 said

> they checked that our application was secure, but they did it in a way that doesn't really prove anything. It's literally a way to mandate all the people who want to get access to data portability APIs to pay at least $700 to this firm for no reason because that security assessment doesn't add any value. It was the most useless security assessment I've ever done.

RP6 similarly felt the assessment did not 'add a great deal of value' but merely concluded that 'if the process had up to that point been really smooth and efficient, then it might not have stung so much. But after going through so much waiting and limbo, it was like, okay, here's another way of slowing things down, putting people off'. RP5 found the CASA verification to be the most time-consuming and difficult part of the process, stating that 'we had to rebuild most of our app, and for a small business like us it's not a light task, on top of the cost of the certification itself'. RP6 added that

> I've seen a few stories and blogs recently from companies that connected to some other Google Workspace APIs, so Google Drive, Gmail etc, saying they're going to

---

[112] "OWASP/ASVS" <https://github.com/OWASP/ASVS>.
[113] OWASP Foundation, "OWASP Application Security Verification Standard (ASVS)" (*OWASP*, 2024) <https://owasp.org/www-project-application-security-verification-standard/>.
[114] App Defense Alliance, "CASA Tiering" (*Cloud Application Security Assessment (CASA)*, March 30, 2023) <https://appdefensealliance.dev/casa/casa-tiering#tiers-calculation>.

> just stop doing that product because the annual security assessment is just too prohibitive.

Looking at publicly accessible online forums where developers were exchanging their experiences of undergoing either the TAC lab assessment or self-assessment, I found more views that aligned with RP6. Developers describe the process of passing CASA as months of back and forth, being asked irrelevant questions, for example, requesting information about their website when they were creating a mobile app, and unclear instructions and documentation, which matches RP2's experience. A developer said the process was so cumbersome they would likely not go through re-verification, and multiple others complained of remaining stuck due to lack of instruction, documentation and correspondence with TAC security. Additional feedback regarding the assessment is required to understand whether it is necessary or is merely prohibitive, but the overwhelming feedback appears to be that the assessment is valueless, time-consuming and expensive.

Looking at whether the process for data sharing on the user side is easy, RP4 pointed out that Google's Portability API consent flow 'could be seen as fearmongering. For the users to agree to use the API, they require the user to click "agree" five different times'. Similarly, RP1 explained that

> It should really be about how you ensure that the people utilising that data, i.e. in our case, us, are trustworthy from the get-go and have the right processes set up from the get-go, not about ensuring that the weight of responsibility is on the user and putting the onus on them, because that's the scary part.

This recognises that the user must understand what data is used and for what purposes, but also that security verification should ensure a minimum level of security, taking the onus off the individual and empowering them to use their data. RP1 went on to describe that there are discrepancies between what Google is demanding third parties include in their consent flows compared to what Google explains when users are connecting to Google-owned services.

> [Google says] we need to ensure that users feel scared appropriately or that they're informed appropriately. You're like, well, you don't do that. You don't put your privacy policy on a page and demand that they read them every time people log in to a new Google property or every six months, right? And that's what you should do if you're going to abide by the same rules.

Therefore, Google should justify the use of excessive consent screens after demanding rigorous security verifications. However, RP6 said that while there may be one too many orange 'scare screens', 'overall, I think we're pretty happy with where the [European] Commission has got the companies to as a starting point'. RP6 again argues that data portability tools have been greatly improved by the DMA and acknowledges that

> There's a really tricky balance to strike between the legitimate need to ensure users know what they're agreeing to and know what company they're engaging with, versus having a streamlined process that makes things easy for people who do know what they're getting themselves into. I think we are not a million miles away from the right balance. I think the next step is accepting what we've got and engaging with the tools as they are.

RP2 acknowledges this ‘tricky balance’ where

> the user has to be aware of what's happening, which is a copy of all their information being moved from Google to another party. So, it makes sense that it's that way. But at the same time, it really seems too much the way they do it right now. There is a screen that explains clearly what's happening, and that could be enough. But when you click continue, there is an orange pop-up that repeats another time the same thing. It just makes it really scary. Then there is the final screen in which the user has to select the scopes of the data that they want to transfer, which is fine. But yeah, there is that screen in the middle that is just exceedingly scary, in my opinion.

RP2 stated that OAuth ‘should be the standard. OAuth is a beautiful protocol that has been developed exactly for this reason […]. It's actually easier for the gatekeeper to just stick to this protocol. They already use this protocol for the single sign-on’. Therefore, it can be concluded that the user consent flow should be simplified, with the verification happening on the back end rather than presenting multiple “scare screens” for users to click through. That said, as RP6 points out, striking the balance between data protection and data sharing is not a ‘clear science’ and further engagement with these tools will be necessary to make fully informed changes.

Of final note regarding the Google Data Portability API, participants expressed discontent that the API still is not real-time and continuous. The API only allows for archived user data transfers, for example, porting a user’s YouTube history, as a one-time transfer meaning users have to re-authorise data transfers. RP1 argues the API ‘doesn't do what it's supposed to do as per the DMA. They know that, too. It's not real-time. It's an archive. They've repurposed their Takeout tool, effectively. And that's pretty lazy because that's actually not what the DMA says’. RP6 said that, despite being verified,

> we haven't done anything with it yet because Google hasn't finished implementing the API. It still only enables one-time transfers, which is the biggest type of friction that they could implement. If a user has to come back and repeat things, then it's pointless. There's no point bothering. We won't build it.

RP1 added that there is no flexibility in how much archival data can be requested, saying that Google only allows for the full archive to be ported. This is too much information, as RP1 explains

> We don't want all of it. You don't know how long someone's been on Google for. For me, it's 2007. That's 17 years’ worth of data. There's no restriction on the scope. Really, you want to say, “actually, we just want the last two years or a year and a half or year. That'll do”. And instead, they're like, “no, you have to have all of it or nothing”.

RP4 called it a ‘firehose’ of data, with RP1 pointing out that despite requiring that developers should only request the minimum amount of data needed via the API, they do not appear to accommodate data minimisation when transferring archival data. RP5 discussed their correspondence with Google regarding the lack of a recursive data transferal option, meaning the ability to set automatic data transfers for a set amount of time, stating that Google appears to be seeking feedback from both developers and the European Commission. RP5 said they suggested implementing the same function as their Google Takeout data download and

transfer tool, where users can export data automatically every two months for a year, but Google ‘didn't want to implement the recursive option as it was in Takeout’. Google shared with RP5 that

> The first idea they showed us required the user to first confirm the data transfer and after 15 days or 30 days, the user has to re-confirm that they want to leave the permission on. If the user does not click on this confirmation, sent via an email from Google, the access is revoked. So, it's like they are trying to put obstacles in place because they are the only ones who are not providing a recursive service.

RP5 explained that Alphabet is cautious about implementing a recursive data transfer option because users often forget about apps they have downloaded and share information with. This needlessly exposes a user and increases the likelihood of an information breach. This points to the tension between increasing contestability and minimising user data sharing for data protection. However, RP1 argues that Alphabet could follow the lead of other gatekeepers like Amazon which plans to show the data sharing prompt once a year, saying ‘annual authorizations make sense.’ Again, if developers undergo security verifications which verify that they can handle the data securely and are not obtaining data for nefarious reasons, additional barriers to data sharing are arguably likely to be tactics to prevent user or developer adoption of portability APIs. That said, all participants acknowledged that Alphabet is already working on improvements to provide real-time and continuous access to user data, therefore the Google Portability API will need to be reassessed when the update is complete.[115]

Meta Portability Tools

While Google’s Data Portability API was the most used by research participants, most participants had overwhelmingly negative feedback on the tools offered by Meta. RP4 disregarded the tools offered by Meta as there is no API available. RP1 described Meta’s offerings as

> terrible. I still don't really understand how it works. We also didn't know on the data side how useful that would be, even though it's Facebook data. It should do pretty well. But again, the tools are just not there on the Facebook side. It's not clear. It's not easy by any means.

RP2 similarly said

> It's a joke. They tell you to submit a form to get in touch with the team, and when you submit the form, you get an email from the team that just says, “Oh, thanks for your interest in the data portability APIs. We'll get back to you as soon as soon as possible. In the meantime, have a look at our documents” and it just provides you with a link to the same document that you filled out the form from and some really outdated documents about the data transfer tool that Facebook developed way back in the day that are really useless. You cannot do anything with that documentation.

[115] Google for Developers (n 58).

RP2 also pointed out that Meta's TYI tool

> is the one that should be DMA compliant, or at least that's what they say. I'm not a lawyer, so I cannot say whether it's compliant or not, but it's definitely a completely different tool from the one that Google, TikTok, or LinkedIn provides. It's just something where you can be listed as a receiver of Facebook data.

This means, importantly, that portability cannot be facilitated in a consent flow like the other gatekeeper tools which, as RP1 said, is the only way portability has a fighting chance.

RP6 had more correspondence with Meta, describing them as 'engaging, open and positive'. However, RP6 ultimately felt that

> as it stands, they haven't really delivered anything. There is no application process or application portal for developers to go through. You can't really apply to get connected and if you did, even then there are a number of drawbacks. So, we spent quite a lot of time engaging with them, but we've stepped back. We gave them a lot of feedback about what improvements we think they should make, and they took this really positively. I think they're in the process of making some big changes. So, I think once those are in place, we'll look to then re-engage with Meta's tool and be listed as a recipient on its download your information tool.

RP5 also had correspondence with Meta but also found that there was very little information to work with as Meta's APIs are still under development. Assessment of Meta's portability tools will likely need to be revisited in future if Meta releases a portability API.

LinkedIn Data Portability APIs

None of the participants have managed to be verified by Microsoft for the LinkedIn Data Portability APIs.[116] RP2 reported that they have been continuously rejected for not proving ownership of their company domain despite sending the documents requested. In fact, when initially applying for verification, RP2 said that while Microsoft requested the company name and registration address, 'they didn't provide any field for us to upload the certificate of registration of the company' yet 'they rejected us because we didn't prove that we were actually that company. And the feedback that they give us was not really clear in terms of what they were actually looking for'. When appealing the decision, Microsoft cited a lack of certificate of company registration which RP2 pointed out was due to their onboarding missing a field to upload it. RP4 also attempted to be verified but ran into similar problems.

> The verification stage required the reviewer to view the company's LinkedIn profile. Our profile was relatively new which seemed to make the reviewer fail our request blocking access. The review timeline said it was 7-14 days which caused a delay when we applied for it.

In a follow-up with RP4 four weeks after the official interview, they state that they are still being rejected for not verifying that their company is legally registered despite 'entering all the information from companies house website which should show it is registered'. RP2

---

[116] LinkedIn, "Additional Terms for The LinkedIn DMA Portability API Programs" (*LinkedIn*, January 18, 2024) <https://www.linkedin.com/legal/l/portability-api-terms>.

equally has had delays appealing rejection, saying that they have waited for more than two weeks with no update regarding their appeal. Microsoft should consider updating their application process and ensuring that their verification forms include all required fields to avoid unnecessary delays.

Amazon Data Portability API

Similarly, none of the participants have been verified by Amazon. While RP1 and 4 spoke highly of the data described in the Amazon Data Portability API[117], RP1 did not apply for verification and RP4 did not pass verification. RP4 said that developers must 'traverse many barriers before being given access'. For the first stage of verification, a business licence must be submitted to Amazon, then developers must undergo security assessments and set up a "Login with Amazon (LWA)".[118] Following this, developers have to contact Amazon to be "allowlisted", and finally the OAuth verification must be set up.[119] RP4 'did not get past the verification stages' and described the process as consisting of 'different hoops that you have to jump through, none of which were particularly easy'.

RP2 described their experience attempting to be verified, which after an initial positive interaction which they thought would lead to being verified, actually ended up putting them off continuing the process.

> After the call, that's actually when things started. They sent us a list of an absurd number of things that we had to prove to them in order to get access to some data. And to be honest, there was so much stuff that we didn't continue the process because it would take us weeks and weeks to provide all that information. And so right now we decided to focus on the other gatekeepers just because it would have taken too long to get verified with Amazon.

RP5 is continuing to apply for verification by Amazon, but also finding that Amazon's security assessment is strenuous, similar to RP2, and requires perhaps more information than is needed, stating that

> we noticed that they are using the same assessment that they use towards their service providers. They treat you like you are offering Amazon services and handling Amazon data, and they are very thorough. But in our situation, some of the checks don't apply because we are not going to serve Amazon any service.

RP5 went on to describe their correspondence with Amazon where they tried to explain that some of their assessments are unneeded.

> As soon as we had a chance to talk with a physical person, we explained that some of the questions or the requirements were not applicable in our case. […] For some questions, we need to schedule a call with them and pass them some cybersecurity information through screen sharing which our cybersecurity expert didn't want to

---

[117] Amazon, "Available Amazon Data Portability LWA Scopes" (*Amazon Developer*, August 12, 2024) <https://developer.amazon.com/docs/amazon-data-portability/available-scopes.html>.
[118] Amazon, "Configure the Amazon Data Portability Service" (*Amazon Developer*, April 16, 2024) <https://developer.amazon.com/docs/amazon-data-portability/intro-configure.html>.
[119] Ibid.

> share with them, of course, for security reasons. But they still want more information. We are at the point of the last few questions of their questionnaire which will be answered through a video call.

Like RP2, RP5 says that the security assessment has taken up a lot of time. Therefore, while the data offered by Amazon was noted by several participants as being useful to their business use cases, the process of verification is overwhelmingly complicated, preventing developers from trying to gain access. Amazon may need to reconsider to suitability of transferring its security assessment from Amazon service providers to assessing data portability requests.

TikTok P*ortability API*

Yet again, none of the participants have been verified by ByteDance for the TikTok Data Portability API. RP2 is in the process of verification but has said that 'TikTok is similar [to LinkedIn] in the sense that it also has been more than two weeks, and I haven't heard anything from them. I have no idea what's happening'. They stated that it is generally hard to understand what ByteDance requires to be verified. RP4 said that 'ByteDance requires the most details about the app that the API will be implemented on' compared to the other gatekeepers. Specifically, they require the design and user flow of the app to be submitted, and the app must be in staging status, which is the post-development testing stage before the app is fully deployed.[120] RP4 said that this is manually reviewed by ByteDance before given approval which slows down the process. RP4 added that the data described in the API documentation is 'limited to just posts the user made, videos the user viewed and messages they have sent or received'. They argued that this is far from representative of the data collected by ByteDance.[121] Thus, while ByteDance representatives said at their compliance workshop that all they need to know is who the company is and whether the company will use the data for the defined scopes, developers are finding that they require the most amount of information out of the gatekeepers.[122] ByteDance should consider simplifying the verification process and re-evaluating the amount of information needed to access the API.

Apple Account Data Transfer web API

None of the participants were verified by Apple for its Account Portability API, but this is largely due to a lack of interest stemming from different perceptions of the data Apple provides. RP4, who attempted verification, stated that according to file guides[123] theoretically, 'the data Apple says they provide through the API is the most comprehensive of

---

[120] TikTok, "Data Portability Application Guidelines" (*TikTok for Developers*, 2024) <https://developers.tiktok.com/doc/data-portability-api-application-guidelines?enter_method=left_navigation>.
[121] TikTok, "Data Types" (*TikTok for Developers*, 2024) <https://developers.tiktok.com/doc/data-portability-data-types/>.
[122] European Commission (n 59).
[123] Apple Inc., "Need Help Understanding Your Files?" (*Data & Privacy*, 2024) <https://privacy.apple.com/file-guides>.

any of the gatekeepers and has in-depth documentation detailing it all'. On the other hand, RP1 said they did not attempt verification because

> there's nothing there, apparently, right? I mean, we scanned over it, but there's nothing there. They say they collect very little and therefore what they have is not *that* useful, just data on the apps a user uses on their iPhone. Given that they are pro-privacy, I'm going to assume that they are telling the truth in that they don't collect any more data on the user.

It is reasonable that if Apple does not collect user information, there is little to port. That said, consulting Apple's App Store privacy policy, Apple states that it collects 'information about your purchases, connected devices, subscriptions, and other activity in the Apple Store app' for personalisation; 'information about your devices and other account information to provide relevant offers for you'; and 'information about your browsing, purchases, searches, and other activity in the Apple Store app to improve the app and to improve and evaluate our services'.[124] The data accessible via this API should be reassessed when more developers have had access to it to evaluate whether Apple is denying developers access to user information.

RP4, when attempting to gain access to the API said that the 'Apple experience was the worst due to the first barrier being a paywall for the developer account'. This is because Apple requires developers to be Account Holders in the Apple Developer Program to access the API, which costs $99 per membership year.[125] This already raises the barrier to entry and arguably is not compliant with the DMA which explicitly states that data portability should be free of charge. Further along the process, RP4 said that the process is seemingly straightforward as there is a contact form to access the API. However,

> We could not reach this contacting stage as we were faced with an error with the [Apple Developer Program License Agreement]. This licencing is required to get on the page to contact Apple for the data portability API. We ensured we had updated all licencing agreements to no avail and contacted Apple support which also did not solve our problem.

RP6 points out that while Apple was a founding member of the Data Transfer Project and points to its membership in the Data Transfer Initiative as evidence that it enables data portability, its API has been 'deliberately applied in the most restrictive way possible so that the absolute bare minimum number of its users can use it. So, I think something doesn't really add up there'. It could be concluded that Apple is putting barriers in place to prevent API access, and the Commission may need to consider the legality of mandating a yearly $99 fee to access an API that is supposed to be free of charge.

---

[124] Apple Inc., "Apple Store App & Privacy" (*Apple Legal*, July 16, 2024) <https://www.apple.com/legal/privacy/data/en/apple-store-app/>.

[125] Apple Inc., "Requesting Portability of Data for Users in the European Union" (*Apple Developer*, 2024) <https://developer.apple.com/support/account-data-transfer-api-eu/>.
Apple Inc., "Become a Member" (*Apple Developer*, 2024) <https://developer.apple.com/programs/enroll/>.

On RQ2) Is there a need to create formal standards or open protocols?

While interviewees were generally well-aligned in their experiences of attempting to access APIs, they did have some different views on standards. On the whole, most participants agreed that API verification should be standardised and handled by an independent body. However, there were some differences in opinion regarding technological standardisation.

Regarding verification, RP2 emphasised that they ‘don't want these verifications to go away’ not only for security but for consumer trust that their company is safe and secure. However, they state that ‘the way it's done right now, it just leads to a massive waste of time’. RP2 says that the OAuth authentication protocol is ‘an amazing protocol, and I think it's already solving everything that needs to be solved in order to facilitate this data portability from one company to a third party with the consent of the user’. However, as each gatekeeper requires vastly different verification assessments, they argue that

> What is missing really is a standardised verification process to access the APIs. Maybe in that case, having a centralised entity that takes care of the verifications would be easy because probably that way you would also only have to be verified once, and then you could request access to all the data portability APIs because, in the end, it should be the same. If you're eligible for one of the data portability APIs, you should also be for the others.

Similarly, RP5 says that they ‘think the solution is for the European Commission to hand out certifications. They should pick a standard. They should have a new office and a register where you go through a standardised procedure’ for API verification. They point out that getting verified individually for each gatekeeper’s portability tool is incredibly onerous which will only get worse ‘because now there are seven with Booking, I believe. But it could be more. We cannot have a year-long procedure for every company that we want to integrate with. It should be one procedure’. RP1 agreed, stating that an improvement for small businesses seeking to gain access to APIs would be if the ‘verification process is adjudicated, maybe even or run by a third party’, meaning gatekeepers ‘don't own the API anymore. And they don't control the API. That would make a lot more sense and feels safer and more secure for startups who are thinking, “Do I take this risk that one day Google might also just shut this down?”’. This question of risk reduction was of central importance to RP6, who sees dependency on gatekeeper APIs are fundamentally problematic.

> There's a question of how much confidence companies like ours can have in these tools. Can we build a business that has full dependency on these APIs as input into our products? I don't know that we can because they can turn them off at any moment. A bit like we've been hearing for years, apps being suddenly kicked off the App Store or the Play Store, and then all of a sudden, their business is dead. In a way, there's an even worse dependency on these APIs because you can be kicked off at the Play Store or the App Store and the Commission can come in and say, “Don't do that”, and you get put back on. And you haven't lost anything apart from potentially some reputational damage. But with an API, you could spend millions acquiring users that connect to the API. The companies could disconnect you and the Commission could

> come along and say, “Reconnect them”. That's all very well, but you've got to start again. So, there's a big vulnerability there.

Because gatekeepers hold the power over their APIs that ‘shape the conditions for app and business development’[126], developers are left vulnerable to API changes or discontinuations. Having the verification process taken out of the hands of the gatekeepers may help to shift this power dynamic. It would make it difficult for gatekeepers to exercise their ‘built-in power to restrict access to APIs or eliminate them entirely’ if a competitor threatens them.[127]

RP1 did point out that the Commission could ‘be inundated with startups wanting to register for data portability’ access but references the example from the UK’s Open Banking scheme, where large banks were mandated to create APIs to allow for new financial services, as an insightful example.

> Open Banking has the same process. Just copy and paste that. That makes sense. Literally copy and paste it, pretty much. It's just a due diligence for “What's your business? Who are you? If something goes wrong, can we find you again?” It holds you accountable. It's just a usual process. We've got these things. You don't need to reinvent them. We could do it that way.

For third parties to access the API in the Open Banking project, companies had to ‘be accredited by the UK’s Financial Conduct Authority. A review concluded this accreditation was one key reason for the success so far of the Open Banking security framework’.[128] This improved security for users whose financial data was being accessed and ensured that banks could not ‘impose obligations on [third party providers] that go beyond what is necessary to ensure customer security’.[129] RP7, however, held a slightly different view regarding centralised approval bodies, stating that

> In the medical device space, there is this concept of notified bodies in Europe. The EU sets regulations, and then there are different private companies actually doing the certification in exchange for money, of course. This is a more positive and more flexible model compared to the US, where there's only one government agency, the [Food and Drug Administration] FDA, and everybody needs to go through them. If they have a backlog of other things to do, let's say, the COVID pandemic, then nothing gets through because all of their efforts are geared elsewhere. In that sense, my preference, based on this, would be to have several institutions that can make that assessment. You don't need to be dependent on one.

The preference here is to have multiple sites of verification, rather than one which is prone to backlog. Relatedly, RP7 suggested that certification bodies could create ‘a paid-for certification scheme’ for companies to obtain ‘a logo of ethical data transfer’. This would mean that consumers could ‘go to any service and if there's this logo, a person would see that and recognise it is part of the good data economy’. This could help redistribute power in the data space, where companies beyond large gatekeepers could be recognised as trustworthy. Finally, another consideration for verification bodies was raised by RP6, who agreed that a

---

[126] Fernando N Van Der Vlist and others (n 29) 16.
[127] Riley (n 4) 100.
[128] Brown (n 9) 119.
[129] Ibid.

‘central independent body that runs approval and verification or much closer monitoring of it from the European Commission’ would be useful but added that gatekeepers will likely need further oversight beyond just API verification, but potentially overseeing API policies.

> [Gatekeepers] are free to set their own rules and policies which is an area that potentially is problematic, because the application process is one thing, but the rules and guidelines they're setting against, that's the question. That's where they can potentially impose restrictions on you or behave threateningly towards you. I think having direct oversight of those rules that they implement or farming out the verification process would be good. But I think there's a risk that the process could be farmed out to the body that isn't truly independent.

This speaks to the same issue found in standards-setting organisations which are prone to industry capture, thus RP6 highlights a relevant risk to be considered if a centralised verification body or multiple bodies were to be set up.

In the Open Banking example, a multi-stakeholder intermediary had to come up with the API standard, data format standards, security standards, and governance arrangements[130], meaning that the data format itself was entirely standardised. This was because the UK’s Competition and Markets Authority found that

> allowing each bank to create their own APIs raised barriers to widespread and timely adoption of open banking by customers and intermediaries. In these circumstances, developers would either have to build applications which were capable of working with many different standards or use a technical service provider to link them up with lots of different banks.[131]

While recognising that gatekeepers continuing to own the entire process of data access is still deemed problematic, participants were almost entirely united in their view that the regulator should not be in charge of establishing the technical tools but could be entrusted to set the standards. Most felt that the main obstacle right now is verification rather than navigating the various APIs themselves. Indeed, RP6 explicitly said that companies can adapt to different APIs. However, RP3 argued that there needs to be ‘a table for the people to discuss. You need to have the small and the big guys getting together and discussing technical grounds in a safe environment’ because as it stands ‘there is no forum to get together. There is no reference design for a common standard. There is no timetable. There are only the ghost shouts of the Commission threatening to fine companies’. The multi-stakeholder process can be seen as a way to shift power out of gatekeeper hands. Bourreau, Krämer and Buiten point out that, in contrast to the model where gatekeepers set up and maintain their APIs

> Another approach would set up a multi-stakeholder process that defines the specifics of the interface, especially for it to adhere to common, public standards [...]. This could be done through formal standardisation organisations, or some other process with regulatory oversight.[132]

---

[130] Ibid, 117.
[131] Ibid, 121.
[132] Bourreau, Krämer and Buiten (n 24) 29.

However, the authors argue that such an approach is incredibly slow as it either requires standards bodies which, as already mentioned, are slow and subject to gatekeeper capture or, in 'the extreme, this approach could result in regulating the gatekeeper like a public utility, with the regulator defining the interface and its standards and monitoring compliance'.[133] The authors do not suggest this approach because it can stifle fast-moving markets and leave too much technical design up to the regulator. RP7 said they do not believe that regulation should name standards 'because if legislation says that everybody needs to adhere to a standard, then it gets really tricky to ever replace that standard. It might be even more difficult to further evolve that standard'. RP7 said there may be some cases where interoperability needs to be encouraged which can be done through a time-capped mandatory standard which can then easily be lifted if it is producing negative effects or if the standard needs updated.

That said, RP3 argues that gatekeepers are being asked to be interoperable and share data without guidance even though

> These technologies are not compatible […] because Facebook is, for example, treating photos in a completely different way from how Apple does it and Google does it. Not only do they not have the same interest and incentive to approximate it, but it would be suicidal for them to do it because this is how they maintain differentiation between their business models.

This is why there needs to be consensus on some technical aspects, argues RP3, so that there is a shared understanding of permissions, consent and data formats.

> There are two components of a standard that should be taken care of to make this trust framework work and be global. One, you need to have the same reference design on the UI, meaning that the user needs to see the traffic light. […] It's semantic. The same language, everybody understands it […] it could be like a sign for deleting the data and a sign for exporting the data. It has four signs, and it needs to be standardised and everyone needs to use it. […] Then the second layer of technicality implementation is to make sure that when the authentication pops up or OAuth2.0, it is bundled with the right of usage. That means that when the user sees a prompt and clicks it, something happens in the back end, or something happens at the logic level of the system. […] It needs to be a minimum set of requirements that everyone is going to respect, and then they can choose which language they want to implement it with. I'm really convinced it's needed, and governments have to play a role in that. The industry itself is not going to do it.

Such a standardised format, RP3 argues, leads to user empowerment 'as opposed to companies leading solution to solution to each other and then never getting together to do anything really scalable'. On the other hand, RP6 disagrees entirely.

> Yeah, I think when it comes to standardisation efforts, my general reaction is I don't think it's necessary. I think we can spend years in workshops trying to decide schemas and standards and common languages and all of these different things. That would be exactly what the gatekeepers want, I suspect. I think it was great that the Commission just went, "Just do it, and then we'll work out what to do with that, what you deliver

[133] Ibid.

> afterwards". I don't think that's a universally held view. I think there are lots of purists out there who would have wanted a perfect standardised uniform solution. But for already existing businesses that needed something now, I think it was the right approach.

So, while RP3 argues for a long-term vision, establishing standardised mechanisms for individuals to control their data, including to whom to share it with and for what purposes, which would need to undergo a multi-stakeholder standardisation approach, RP6 argues for a more pragmatic approach. RP6 advocates for developers to engage with the current tools as they exist and demand change in areas where it makes sense, for instance at the verification level. Both approaches lend themselves to their own vulnerabilities. While standardisation is slow and can be easily coopted by incumbents, reliance on gatekeeper-owned and run APIs leaves businesses incredibly vulnerable and runs the risk of only facilitating complementary products that remain dependent on incumbent platforms rather than industry-shifting innovations. Additionally, standards, in the long run, would likely level the playing field and facilitate easier control for individuals over their data, thus reducing dependencies on large firms. On the other hand, RP6's approach is more flexible, allowing firms to create their own portability APIs and end products, with the best solutions likely to be adopted more widely.

Somewhere in between these two opposing views sat RP4, who argued that data portability itself may have a data interoperability effect, meaning when 'data exchanges between different services [occur] in real-time'.[134] Because at present, data portability faces the challenge that each gatekeeper holds data in different formats for different business models, RP4 stated that

> when you ingest your Google and your Facebook and your TikTok, and you've got that in, let's say, the filing cabinet, you then have to normalise that to make value of it. Because as I say, it's three videos from three different sources rather than, "Here's what I got from Google, here's what I got from Facebook". […] So essentially, you have this big data model for a person, which then allows you to normalise and when you push it back out again, it becomes more interoperable. […] The source becomes less important and more about what interesting things can I build on that aggregated data. It doesn't matter whether it's come from Google or TikTok or whatever.

This normalisation process makes the data readable and useable beyond individual platforms, thus increasing its interoperability. RP4 also discussed the use of federated open IDs, which is a portable identifier rather than an identifier attached to a single platform. If one platform shuts down the user can carry the identifier to another platform which reduces dependencies on a single platform. This approach has the benefit of not requiring a long-standardisation process and could in the long term reduce dependencies on incumbent platforms if users can utilise data portability more efficiently. A major caveat to this approach is that it largely depends on widespread user adoption and users abandoning popular sign-in protocols via Google or Facebook.

[134] Ibid, 13.

Finally, though the DMA is a European regulation, it is hoped that there will be a so-called Brussels Effect[135] where DMA-established tools can be useful for those not residing in the EU. RP6 explicitly said

> I think clearly the outcome we would all want to see is that all of these tools are available globally because any company that's like ours operating this space wants to have global users. And so, you don't want to have this disparate patchwork of features that you have to deliver for some users and not others. [… Making these portability APIs] I think is beneficial for the gatekeepers. I think it's beneficial for developers who don't want to connect to loads of different APIs. I think that's the bit where I argue for standardisation in terms of geography rather than formats and technical solutions.

Article 6(9) likely will help businesses grow and scale far more if they are able to reach global audiences.

Conclusion

To conclude, in answering RQ1, there remain significant barriers for developers to access the APIs offered by the gatekeepers. While Alphabet currently leads in terms of accessibility, participants were clear that the process is slow, and that security verification is a significant barrier. While it can be challenging to assess from the outside whether API restrictions in the name of security and privacy are legitimate or merely ways to cut off data access from competitors, this research illustrates that Alphabet may be using security assessments to put developers off attempting to access its API. While participants agreed that security checks should be in place, they had an overwhelmingly negative experience with TAC Security which asked for redundant information, unclear instruction and slow communication. Therefore, the access policies and vetting procedure were not made clear. That said, pre-verification data access for small developers or apps in development and testing was seen as a positive that other gatekeepers should consider.

The other gatekeepers should seek to improve accessibility significantly. Though participants have attempted to gain access, no participant could access any other gatekeeper's data portability tools. Gatekeepers have both been unclear in explaining to developers what should be submitted to be verified and have not been communicative with developers trying to access the APIs. Almost all participants felt that verification for API access should be handled by an independent third party to standardise the process and take liability from gatekeepers' hands.

The data portability tools are still in their infancy, with Meta and Alphabet working to improve their tools to allow for data transfers programmatically. Thus, in response to RQ2, it is too soon to argue for creating specific standard protocols. It appears most participants feel that developers can navigate the different APIs offered by gatekeepers and that this is preferable to fixed standards at this stage. Indeed, most participants felt that verification is the biggest hurdle and that it may be beneficial to have an independent body handle this process.

---

[135] Anu Bradford, *The Brussels Effect* (Oxford University Press 2019) <https://doi.org/10.1093/oso/9780190088583.001.0001>.

Before major conclusions regarding the portability tools can be made, more developer feedback will be needed as the tools become more widespread. However, this research highlights a dilemma; there is a need for more developer feedback to understand the enforcement of Article 6(9), but gatekeepers are making API access cumbersome meaning that there is unlikely to be widespread adoption from which feedback can be gleaned. Additionally, developers see the multistakeholder standardisation process as slow and can result in gatekeeper capture, but there may need to be technical dialogue to improve API access in a way that protects the security and privacy of users. Therefore, the Commission may need to consider intervention at the verification level and the author concludes that this study will need to be reevaluated when developer tools have released improvements, particularly Google and Meta's proposed improvements.

References

Amazon, "Configure the Amazon Data Portability Service" (*Amazon Developer*, April 16, 2024) <https://developer.amazon.com/docs/amazon-data-portability/intro-configure.html>

——, "Available Amazon Data Portability LWA Scopes" (*Amazon Developer*, August 12, 2024) <https://developer.amazon.com/docs/amazon-data-portability/available-scopes.html>

——, "Amazon Data Portability Overview" (*Amazon Developer*, 2024) <https://developer.amazon.com/docs/amazon-data-portability/overview.html>

App Defense Alliance, "CASA Tiering" (*Cloud Application Security Assessment (CASA)*, March 30, 2023) <https://appdefensealliance.dev/casa/casa-tiering#tiers-calculation>

Apple Inc., "Account Data Transfer" (*Apple Developer Documentation*, 2024) <https://developer.apple.com/documentation/AccountDataTransfer>

——, "Become a Member" (*Apple Developer*, 2024) <https://developer.apple.com/programs/enroll/>

——, "Need Help Understanding Your Files?" (*Data & Privacy*, 2024) <https://privacy.apple.com/file-guides>

——, "Requesting Portability of Data for Users in the European Union" (*Apple Developer*, 2024) <https://developer.apple.com/support/account-data-transfer-api-eu/>

——, "Apple's Non-Confidential Summary of DMA Compliance Report" (European Commission 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>

——, "Apple Store App & Privacy" (*Apple Legal*, July 16, 2024) <https://www.apple.com/legal/privacy/data/en/apple-store-app/>

Article 29 Data Protection Working Party, "Guidelines on the Right to Data Portability" (European Commission 2016) WP 242 rev.0 <https://ec.europa.eu/newsroom/article29/items/611233/en>

Berman A, “Industry, Regulatory Capture and Transnational Standard Setting” (2017) 111 AJIL Unbound 112 <https://doi.org/10.1017/aju.2017.29>

Bernal J, “Private Sector Trust in Data Sharing: Enablers in the European Union” (2024) 6 Data & Policy <https://doi.org/10.1017/dap.2024.20>

Bloch J, “A Brief, Opinionated History of the API” (New York, United States of America) <https://www.infoq.com/presentations/history-api/>

Bodle R, “Regimes of Sharing: Open APIs, Interoperability, and Facebook” (2011) 14 Information Communication & Society 320 <https://doi.org/10.1080/1369118x.2010.542825>

Booking – Online intermediation services (Case DMA. 100019) Commission Decision [2024] <https://ec.europa.eu/competition/digital_markets_act/cases/202442/DMA_100019_191.pdf> .

Bourreau M, Krämer J and Buiten M, “Interoperability in Digital Markets” (Centre on Regulation in Europe (CERRE) 2022) <https://cerre.eu/publications/interoperability-in-digital-markets/>

Bowyer A and others, “Human-GDPR Interaction: Practical Experiences of Accessing Personal Data” (2022) 106 CHI Conference on Human Factors in Computing Systems 1 <https://doi.org/10.1145/3491102.3501947>

Bradford A, *The Brussels Effect* (Oxford University Press 2019) <https://doi.org/10.1093/oso/9780190088583.001.0001>

Brown I, “The Technical Components of Interoperability as a Tool for Competition Regulation” (OpenForum Academy 2020) <https://www.openforumeurope.org/wp-content/uploads/2020/11/Ian_Brown_The_technical_components_of_interoperability_as_a_tool_for_competition_regulation.pdf>

——, “The UK’s Midata and Open Banking Programmes: A Case Study in Data Portability and Interoperability Requirements” (2022) 2022 Technology and Regulation <https://techreg.org/article/view/11539>

——, “Private Messaging Interoperability in the EU Digital Markets Act” (2022) <https://openforumeurope.org/wp-content/uploads/2022/11/Ian_Brown_Private_Messaging_Interoperability_In_The_EU_DMA.pdf>

Bruns A, “After the ‘APIcalypse’: Social Media Platforms and Their Fight against Critical Scholarly Research” (2019) 22 Information Communication & Society 1544 <https://doi.org/10.1080/1369118x.2019.1637447>

Cotton IW and Greatorex FS, “Data Structures and Techniques for Remote Computer Graphics” [1968] Association for Computing Machinery <https://doi.org/10.1145/1476589.1476661>

Data Transfer Initiative, “Data Transfer Initiative Home Page” (*Data Transfer Initiative*, 2024) <https://dtinit.org/>

Doctorow C, *The Internet Con: How to Seize the Means of Computation* (Verso Books 2023)

ETSI, “What Does Membership Cost?” (*ETSI*) <https://www.etsi.org/membership/dues>

European Commission, “Compliance Reports” (*Digital Markets Act (DMA)*, 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>

——, “DMA Designated Gatekeepers” (*Digital Markets Act (DMA)*, 2024) <https://digital-markets-act.ec.europa.eu/gatekeepers_en>

——, “Compliance with the DMA: Meta” <https://webcast.ec.europa.eu/compliance-with-the-dma-meta-2024-03-19>

——, “Compliance with the DMA: Amazon” <https://webcast.ec.europa.eu/compliance-with-the-dma-amazon-2024-03-20>

——, “Compliance with the DMA: Bytedance” <https://webcast.ec.europa.eu/compliance-with-the-dma-bytedance-2024-03-22>

——, “Commission Starts First Proceedings to Specify Apple’s Interoperability Obligations under the Digital Markets Act” (*Digital Markets Act (DMA)*, September 19, 2024) <https://digital-markets-act.ec.europa.eu/commission-starts-first-proceedings-specify-apples-interoperability-obligations-under-digital-2024-09-19_en>

Evans PC and Basole RC, “Revealing the API Ecosystem and Enterprise Strategy via Visual Analytics” (2016) 59 Communications of the ACM 26 <https://doi.org/10.1145/2856447>

Fenwick M, Jurcys P and Minssen T, “Data Portability Revisited: Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow” [2024] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4475106>

Flew T, “The Platformized Internet: Issues for Internet Law and Policy” [2019] Journal of Internet Law <https://eprints.qut.edu.au/129830/>

Gillespie T, “The Politics of ‘Platforms’” (2010) 12 New Media & Society 347 <https://doi.org/10.1177/1461444809342738>

Goldstine H and Von Neumann J, “Planning and Coding of Problems for an Electronic Computing Instrument: Report on the Mathematical and Logical Aspects of an Electronic Computing Instrument Part II Vol III” (Princeton University Institute for Advanced Study 1948)

Google, “How to Download Your Google Data” (*Google Account Help*, 2024) <https://support.google.com/accounts/answer/3024190?hl=en>

——, “When Is Verification Not Needed” (*Google Cloud Platform Console Help*, 2024) <https://support.google.com/cloud/answer/13464323>

Google for Developers, “Data Portability API Release Notes” (*Data Portability API*, 2024) <https://developers.google.com/data-portability/docs/release-notes>

——, “Introduction: Develop Apps Using the Data Portability API” (*Google for Developers*, 2024) <https://developers.google.com/data-portability/user-guide/introduction>

——, “Restricted Scope Verification” (*Google Identity*, July 16, 2024) <https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification?hl=en>

Graham-Harrison E and Cadwalladr C, “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach” *The Guardian* (March 17, 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Heft-Luthy S, “Introducing TikTok’s Data Portability API” (*TikTok for Developers*, 2024) <https://developers.tiktok.com/blog/2024-introducing-tiktok-data-portability-api>

Helmond A, “The Platformization of the Web: Making Web Data Platform Ready” (2015) 1 Social Media + Society 205630511560308 <https://doi.org/10.1177/2056305115603080>

LinkedIn, “LinkedIn Pages Data Portability API Application Review and Developer Support” (*LinkedIn Help*, 2024) <https://www.linkedin.com/help/linkedin/answer/a6216629>

——, “Additional Terms For The LinkedIn DMA Portability API Programs” (*LinkedIn*, January 18, 2024) <https://www.linkedin.com/legal/l/portability-api-terms>

Lomborg S and Bechmann A, “Using APIs for Data Collection on Social Media” (2014) 30 The Information Society 256 <https://doi.org/10.1080/01972243.2014.915276>

McIntyre DP and Srinivasan A, “Networks, Platforms, and Strategy: Emerging Views and Next Steps” (2016) 38 Strategic Management Journal 141 <https://doi.org/10.1002/smj.2596>

Meta, “Accessing and Downloading Your Facebook Information” (*Facebook Contact Forms*, 2024) <https://www.facebook.com/help/contact/2032834846972583>

——, “Download a Copy of Your Information on Facebook” (*Facebook Help Centre*, 2024) <https://www.facebook.com/help/212802592074644/>

Microsoft, “Member Data Portability (Member)” (*Microsoft Learn*, February 5, 2024) <https://learn.microsoft.com/en-us/linkedin/dma/member-data-portability/member-data-portability-member/?view=li-dma-data-portability-2024-08>

——, “Non-Confidential Version 1 Microsoft Compliance Report – Annex 11 – LinkedIn (Online Social Networking Service)” (European Commission 2024) <https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports>

Morland W, “What’s New With Data Portability and Our Transfer Your Information Tool” (*Meta*, October 22, 2022) <https://developers.facebook.com/blog/post/2022/10/18/data-portability-and-our-transfer-your-information-tool/>

Morton FMS and others, “Equitable Interoperability: The ‘Supertool’ of Digital Platform Governance” (2023) 40 Yale Journal on Regulation <https://www.yalejreg.com/print/equitable-interoperability-the-supertool-of-digital-platform-governance/>

Morton FS and others, “Stigler Committee on Digital Platforms: Market Structure and Antitrust Subcommittee” (The University of Chicago Booth School of Business 2019) <https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report>

Nicholas G and Weinberg M, “Data Portability and Platform Competition: Is User Data Exported From Facebook Actually Useful to Competitors?” (Engelberg Center on Innovation Law and Policy 2019) <https://www.law.nyu.edu/sites/default/files/Data%20Portability%20and%20Platform%20Competition%20-%20Is%20User%20Data%20Exported%20From%20Facebook%20Actually%20Useful%20to%20Competitors.pdf>

“OAuth Community Site” <https://oauth.net/>

OWASP Foundation, “OWASP Application Security Verification Standard (ASVS)” (*OWASP*, 2024) <https://owasp.org/www-project-application-security-verification-standard/>

“OWASP/ASVS” <https://github.com/OWASP/ASVS>

Patel N, “Twitter Granted Patent on Pull-to-Refresh, Promises to Only Use It Defensively” *The Verge* (May 21, 2013) <https://www.theverge.com/2013/5/21/4350826/twitter-pull-to-refresh-patent-innovators-patent-agreement-announced>

“Photo Storage” (*Photobucket*) <https://photobucket.com/>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/01.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ 2 265/1.

Riley C, “Unpacking Interoperability in Competition” (2020) 5 Journal of Cyber Policy 94 <https://doi.org/10.1080/23738871.2020.1740754>

——, “A Framework for Trusted, Safe Third-Party Data Transfers” (*Data Transfer Initiative*, November 7, 2023) <https://dtinit.org/blog/2023/11/07/framework-trust>

——, “Data Transfer Initiative Members Apple and Google Introduce New Photo and Video Transfer Tool” (*Data Transfer Initiative*, July 10, 2024) <https://dtinit.org/blog/2024/07/10/DTI-members-new-photo-video-tool>

Sconiers-Hasan M, “Application Programming Interface (API) Vulnerabilities and Risks” (Carnegie Mellon University 2024) <https://insights.sei.cmu.edu/library/application-programming-interface-api-vulnerabilities-and-risks/>

Sharma C, “The Present and Future of Data Portability: A Collected Volume of Independent Scholarly Research” (The Data Transfer Initiative ed, The Data Transfer Initiative 2024) <https://dtinit.org/assets/DTI-Data-Portability-Compendium.pdf>

Snodgrass E and Soon W, “API Practices and Paradigms: Exploring the Protocological Parameters of APIs as Key Facilitators of Sociotechnical Forms of Exchange” [2019] First Monday <https://doi.org/10.5210/fm.v24i2.9553>

Stucke ME, “The Relationship between Privacy and Antitrust” [2022] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.4042262>

TAC Security, “TAC Security” (2024) <https://tacsecurity.com/>

TikTok, “Data Portability Application Guidelines” (*TikTok for Developers*, 2024) <https://developers.tiktok.com/doc/data-portability-api-application-guidelines?enter_method=left_navigation>

——, “Data Types” (*TikTok for Developers*, 2024) <https://developers.tiktok.com/doc/data-portability-data-types/>

Toropainen S, “The Right to Data Portability in the Fair Data Economy” (Sitra 2023) <https://www.sitra.fi/en/publications/the-right-to-data-portability-in-the-fair-data-economy/>

Van Der Vlist FN and others, “API Governance: The Case of Facebook’s Evolution” (2022) 8 Social Media + Society <https://doi.org/10.1177/20563051221086228>

Van Der Vlist FN and Helmond A, “How Partners Mediate Platform Power: Mapping Business and Data Partnerships in the Social Media Ecosystem” (2021) 8 Big Data & Society 205395172110250 <https://doi.org/10.1177/20539517211025061>

Zhang N and others, “Web APIs: Features, Issues, and Expectations – A Large-Scale Empirical Study of Web APIs from Two Publicly Accessible Registries Using Stack Overflow and a User Survey” (2022) 49 IEEE Transactions on Software Engineering 498 <https://doi.org/10.1109/tse.2022.3154769>