Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Unpacking interoperability in competition

Chris Riley

To cite this article: Chris Riley (2020) Unpacking interoperability in competition, Journal of Cyber Policy, 5:1, 94-106, DOI: 10.1080/23738871.2020.1740754

To link to this article: https://doi.org/10.1080/23738871.2020.1740754

Published online: 15 Mar 2020.

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 1, 94–106
https://doi.org/10.1080/23738871.2020.1740754

Routledge
Taylor & Francis Group

Unpacking interoperability in competition

Chris Riley

Mozilla, San Francisco, CA, USA

ABSTRACT

Growing centralisation in the tech sector is raising global governmental concern, and the winds of change are blowing. Interoperability – in this context, the ability of internet-connected technologies to work together, for example by exchanging data and accessing functions remotely – is gaining traction as a component of the coming regulatory and legislative reforms. Against a backdrop of rapidly evolving law and technology, this paper examines how interoperability fits within the existing landscape for competition law, and where it may be interpreted to be applicable to the complex system of data exchanges whose emergence we call the internet.

ARTICLE HISTORY
Received 19 September 2019
Revised 25 February 2020
Accepted 26 February 2020

KEYWORDS
Interoperability; competition; competition law

Introduction

Interoperability is a central concept in the history of communications networks. Imagine a world where you couldn't call another person unless you both used AT&T for your wireless service. Yet the technical and economic evolution of the internet took a different path. Whether motivated by advertising-driven business models, two-sided digital platform markets, the rapid pace of innovation as compared to negotiations within standards bodies or regulatory processes, or any number of other causes, the standard assumption today is that you talk to Facebook users via Facebook, iMessage users through your iOS devices and Skype users on Skype. That creates a powerful lock-in effect – natural forces pushing towards greater centralisation, or competition 'for' the market rather than 'in' the market (George J. Stigler Center 2019).

Competition policymakers are fully aware of this dynamic and increasingly, analyses and reports indicate that the future direction of regulatory travel will be towards the promotion of interoperability. In April 2019, the European Commission released an Expert Report, commissioned by the Directorate-General for Competition (DG-COMP) and written by three outside academic advisors, entitled 'Competition policy for the digital era'. The report used the word 'interoperability' 105 times and defined three separate types of interoperability for purposes of understanding competition in the digital economy: 'protocol interoperability', 'data interoperability', and 'full protocol interoperability' (Crémer, de Montjoye, and Schweitzer 2019). The United Kingdom's Competition and Markets Authority added another term in its December 2019 interim report on digital advertising: 'content interoperability' (CMA 2019).

CONTACT Chris Riley mchris@gmail.com

As a source of expert input to DG-COMP, the expert report will influence future policy and legislative actions by the European Commission in its new mandate. Similarly, the report of the UK's Digital Competition Expert Panel (2019) (the 'Furman Review') will influence future considerations of the UK government's Competition and Markets Authority; indeed, the CMA's interim report on digital advertising reflects many elements of the Furman Review. And the working group report from the Stigler Center at the University of Chicago Booth School of Business will join with other academic work in the United States to influence the Federal Trade Commission, the Department of Justice and Congress as those bodies consider how best to approach competition online (George J. Stigler Center 2019).

The focus of this paper is on interoperability in the context of digital platforms, defined, for example, in the report of the US Commerce Department's Digital Economy Board of Advisors (DEBA 2016). While interoperability also applies to hardware, networking protocols and many other pieces of the information and communications technology stack, the greatest focus in tech competition debates today is on this software and services internet-connected layer, the world of apps and social networks and the World Wide Web.

Within the digital platform context, this paper will unpack the term 'interoperability' to explore what this regulatory evolution may entail in practice. 'Interoperability', as used here, is a broad concept, encompassing both the 'content interoperability' and 'protocol interoperability' frames of the CMA and EC experts' reports, and more; it's meant to cover generally the ability of internet technologies to work together. This includes horizontal interoperability – messaging services that can send messages to services run by other companies, for example – and vertical interoperability – downstream technologies that can incorporate content and data of digital platforms, and/or generate content and data that then goes into the platforms. Interoperability in this broad sense can be symmetrical, as with communication standards like SMS (text messaging), where both parties agree to use identical formatting so that content from one service can be used in another without modification, or it can be asymmetrical, where a platform service offers an Application Programming Interface (API) or some other mechanism by which third parties can push or pull data of various forms to or from the platform.

Interoperability and law

Interoperability is a strange beast when considered against the historical backdrop of antitrust law and competition. Generally, businesses are not obligated by law to work with other businesses. A well-established limit to this principle is the 'essential facilities doctrine', in which bottlenecks in a market, controlled by firms with significant power, can be used as barriers to market entry in a manner that constitutes illegal monopolisation.[1] Related to this, in American law, one widely recognised 'far reach' of legal limits to refusals to deal is the *Aspen Skiing* case (1985), in which the decision to terminate a joint venture without a clear economic justification was upheld by the US Supreme Court as an illegal act of monopolisation. In recent years, the essential facilities doctrine has fallen out of favour with courts, and *Aspen Skiing* (while not overturned) has frequently been distinguished as an outlier. Thus, it would seem to be a stretch to expect success in contending, for example, that Facebook's News Feed constitutes an essential facility, or that failing to provide full access to it constitutes an illegal refusal to deal.

Another applicable theory under antitrust law is tying. In the context of digital platforms, effective tying would mean that two different services offered by the same provider must be used together, and neither can be used in the same way with a functional competitor offered by another (Sharma 2020). Tying was at stake in the high-profile antitrust investigations into Microsoft over the technical interconnections between Windows and Windows Server (Microsoft Corp. v Commission of the European Communities 2007). In the context of interoperability, two services offered by the same provider can be connected through private APIs – interoperability interfaces not made available for use by third parties – in contrast to public, transparent, third-party-facing APIs that can, in theory, be as usable by others as by the platform operator.

Communications law offers the opposite paradigm to antitrust, in particular through its embrace of common carrier doctrine. Sections 201 and 202 of the Communications Act of 1934 require service to be provided on reasonable terms to all customers, deriving from the law over railroads and interstate commerce, itself derived from old English common law applicable to businesses whose purpose is to convey goods on behalf of people (47 US Code § 201-02; Bettilyon 2017). In many ways under the law, digital platforms are given special status as intermediaries, distinguishing, for example, a service like Netflix, which was designed to deliver professional video content, from a service like YouTube, which was designed to host user-uploaded videos and make them available to other users (although in practice any such lines blur easily). Some legal scholars have proposed applying comparable communications law principles to the practices of internet intermediaries, even though their technical functions differ substantially from the operator of a railroad or a phone network (Pasquale 2008).

Neither antitrust, nor communications offer a perfect legal paradigm to capture the internet and the digital platform economy. This, more than anything, explains the efforts by multiple governments around the world over the past few years to come to grips with the challenges posed by increasingly centralised markets in technology.[2]

Interoperability and data portability

One way in which the competition dynamics of interoperability have emerged into law is through the related concept of 'data portability'; the two share many features in common, yet also have many differences. Data portability is one of the eight fundamental digital rights established in the European Union's General Data Protection Regulation (GDPR), and as a concept, has been well known and discussed within the technical community for decades. Data portability, as a principle, says that your data is yours, and even when you provide data (such as your phone number, but also your messages, status updates, etc.) to a platform, you do not lose the right to take back possession of the data – to 'port' it out of the platform so that you can put it to other purposes.

Data portability thus serves two potential purposes. One comes from the realm of privacy: you 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.

The differences between data portability and interoperability become clear when thinking about how competition emerges in practice. In particular, data portability doesn't port networks, only data. Even where a user of a social network can port their 'social graph' of connections to a competing service, one user can't force all of their connections to also switch services. Effective interoperability, with its real-time functionality, overcomes that gap by allowing users to send messages through the underlying platform; it represents a more dependent form of competition, but one that doesn't require amassing a comparable baseline network and data store to provide the same levels of access.

The Data Transfer Project (DTP) reflects something at the intersection of these two ideals (Data Transfer Project Overview 2018). The white paper articulating the effort makes clear its competitive ambition.[3] DTP is designed to make the offline, one-time porting of a user's data and experience from one service to another as streamlined as possible, while making user security, privacy and agency considerations a priority. In a world where effective competition already exists, DTP would serve as a very compelling solution to sustain it.

The technical mechanisms of DTP focus on asynchronous, batch transfers of user data – one-time operations, not the sort of real-time interoperability transactions that power the internet we have today. The previously cited economic reports shaping the future of competition policy reflect the distinctions between these two functions and recognise, rightly, the merits of both as components of a competitive internet ecosystem.

Interoperability and the internet

Digital applications ('apps'), services, networks and other technologies interact with each other in complex ways. Leaving behind the 'stack' once reflecting layers of internet technologies, as illustrated by the seven-layer Open Systems Interconnection (OSI) model, today's ecosystem looks far more like a cloud than an hourglass. Apps are built with libraries specific to individual operating systems, incorporating accounts and services from many other parties, creating a massively interconnected, complex system that presents numerous points of technical intersection, each in the form of a transfer of data or a remote procedure call.

These interactions, when they work well, contribute to the relative ease of market entry and the vibrancy of competition when it's at its best online. It's far easier, for example, to implement Google sign-in than to develop, test, ship and maintain your own account creation and authentication system.[4] The key points of interconnection are often controlled by one or a few powerful companies, putting them in a position to impede interoperability and competition by exercising gatekeeper behaviour (DEBA 2016).

Healthy interoperability across the complex technical interconnection points of the internet means that new services can enter the market and compete with relative ease. Unhealthy interoperability means unduly and artificially expensive market entry, or a context where rising competitors – succeeding in a setting of low-cost entry and growth – can be stifled at will by a dominant party fearing market disruption.

The future of competition and antitrust will be far more complicated than the present. We have decades (or centuries) of understanding in the context of legal contracts governing prices and terms of deals between businesses, and expertly trained lawyers and judges who understand the relevant nuances and can compare them to existing precedents.

However, gauging whether a change to the permissions and usage policies of an Application Programming Interface constitutes a thoughtful response to a legitimate security concern, or an anticompetitive act designed to repress a competitor, is a far different challenge.

The norms and standards of good behaviour here are far from settled, and I won't purport to offer a complete solution in this paper. Instead, I will describe six different ways in which the concept of interoperability can be seen in practice, and explain how each presents technological choke points, which become opportunities to promote or to impede competition. These six are not intended to be a complete characterisation of the entirety of technical interoperability or possible gatekeeper choke points for competition online, but they collectively represent a large range of competitive concerns present today.

Standards bodies

At its core, the internet is built on technical standards. Standards align the products and services of multiple companies to allow for effective horizontal and vertical compatibility and technical interoperability. Electrical plugs offer the most effective illustration of the value of standards: houses within a country are all built using the same electrical outlets, so all devices can use the same outlets, and designers of electrical products know how to build their products. Differences in standards across countries are easily handled through universal adapters.

The downside, of course, is that updating a standard can be complicated. Sometimes, backward compatibility can be preserved to reduce associated cost and effort. For example, when electrical plugs in the United States added a third, ground plug, the third plug was added in such a way that two-prong plugs would still work in three-prong outlets (though three-prong plugs require adapters to work with two-prong outlets). Meanwhile, USB-powered electrical devices have grown so commonplace that hotels frequently make USB power ports available next to standard electrical outlets, although the USB standard continues to evolve.

Standards power technology far beyond the physical device layer. Internet protocol (IP) is a standard, as is hypertext transfer protocol (HTTP), both under the auspices of the Internet Engineering Task Force (IETF). As standards move away from the physical layer and towards more rapidly evolving applications and purposes, the challenges of maintaining a central standard and ensuring clear adherence to the standard grow. Messaging protocols illustrate this dynamic well; there are established standards, most notably XMPP, yet popular messaging services like WhatsApp and Signal use proprietary protocols that do not allow for easy interconnection (see e.g. Marlinspike 2016).

Drifting away from standards is one dimension of competitive concern; a more subtle source of concern arises from the possibility that a powerful company could co-opt, undermine 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. In this context, even where interoperability would exist in theory, an uneven cost would be

introduced into the competitive process, or perhaps a tax would be a better metaphor – a sacrifice in functionality paid by competitors to the benefit of the dominant firm.

Actions that undermine standards bodies and processes may be hard to identify and prove in practice, but the harm that such abuse poses to effective and meaningful interoperability makes the consideration of standards processes and outcomes worthwhile in the context of competition.

Application programming interfaces (APIs)

Where standards bodies constitute the core of the internet, APIs are the next layer out. They reflect the heart of what it means to be a 'platform' in the digital world – to offer access to key data and functionality of a service in order to unlock downstream markets. Or, in less economic terms, encouraging others to innovate on top of existing systems and combine them with new ideas to make something even better. APIs are the primary mechanism for this efficient repurposing of the non-rivalrous goods of data and networks. They allow the platform operator full control over the extent of data and functionality made available, empowering the creation of both technical and legal constraints on access. Given their breadth of utility, APIs are the most common, and also the most complex, form of interoperability and represent both the biggest opportunity for pro-competitive actions and the biggest potential source of competitive harm.

A third-party-facing API turns a service into a platform. APIs work by establishing a mechanism for remote services to request something of the platform, loosely described as either data to be provided by the platform, or an operation to be performed by the platform (Bock 2015). So, a storage platform could establish a basic API to allow applications to read data from the remote storage, and another to allow data to be written to the remote storage.

APIs can be 'open' or 'restricted', a term which may seem pejorative but in fact describes most APIs. A truly 'open' API can be called by any remote service at any point, under any circumstances, and the platform will strive to fulfil the request; consequently, no data of any privacy or security significance would be made available through an open API, and the commercial significance of such APIs is limited. APIs are often authenticated – ensuring that the service accessing the API is legitimate and not fraudulent or malicious, and where applicable, validating the identity of the user of the platform (in the typical circumstance where a user is requesting data from the user's account with the platform through a third-party application or service). APIs are typically limited both technically and through usage policies; technical limits take the form of rate limits on the amount of data that can be transmitted over a certain period of time (to minimise fraud and other harmful behaviour), and policy limits can help to ensure the platform's user experience and expectations are preserved.

Public-facing APIs are often documented thoroughly, as their primary value-add for the platform is in empowering third parties to deliver added value to the platform by extension.[5] After all, if a Facebook app developer builds a great game that can only be used by Facebook users, that reinforces the value proposition for Facebook. Consequently, many natural incentives within the API ecosystem encourage broad adoption and use of APIs by third parties. In this optimistic interpretation, APIs represent a vector for extremely low-cost market entry and incredible opportunities for competition. Platforms are in

some sense sharing access to the valuable repositories of data and networks they have built, and in doing so, are making it much easier for third parties to reach large volumes of users.

The flip side of the coin comes in with the built-in power to restrict access to APIs or eliminate them entirely. APIs unlock downstream innovation and can seed the growth of competitors, but the platform owns the only master key. In some sense, this constitutes a deep theoretical challenge to Clayton Christensen's theory of disruptive innovation (Bower and Christensen 1995). If a disruptive market emerges downstream of the platform, or is dependent on access to the platform's network or data, the platform can nip it in the bud by closing off access to its APIs.

This isn't merely a theoretical concern. The past few years have seen substantial allegations of competitive harm as a result of major platforms making changes to their APIs (see e.g. Constine 2018a; Constine 2018b; Van der Mersch 2016; Lomas 2015). These changes were justified by the platforms under a number of different auspices, particularly security and privacy benefits. Certainly, some of those justifications have been valid, at least with respect to their nominal objectives. However, it's hard to measure the harm to competition of a change to platform APIs (Feld 2018). It's even harder to make an objective decision as to the net economic and social benefits of the action.

This dynamic, the difficulty of gauging changes to APIs, is on display on a regular basis. Facebook's 'Cambridge Analytica' scandal arose from an overly permissive API. The company's 'Graph 1.0' API allowed users to authorise a third party to access some information regarding their Facebook 'friends' without the direct permission of those individuals. Facebook therefore changed the API to offer less information and continued in that vein to deprecate its 'publish_actions' API in a manner that proved devastating for some downstream services (Barrett 2018).

We've already seen one successful legal challenge regarding API practices. In 2012, the Federal Trade Commission reached a settlement with Google, in which the company agreed to change the policies for its AdWords API, which had previously prohibited third parties from running the same campaigns over Google's network and other ad networks (Search Marketing Daily 2017). The settlement forced Google to contribute to a better downstream ecosystem for advertising, and the growth of that ecosystem in return benefited Google as a platform, prompting the company to extend the practice even after its legal obligation under the settlement expired (Sucherman 2017).

APIs, and the frequent technical and policy changes that are made to them, are a nuanced and challenging part of the interoperability puzzle. It's difficult, and yet critical, for competition regulators to be in a position to examine changes to APIs and make a determination as to whether they are valid for security, privacy, or other benefits, or whether those other asserted rationales are mere covers for practices that are properly interpreted as illegal anticompetitive behaviour.

Web (and device, and platform) compatibility

When operating properly, standards bodies can establish a baseline of effective interoperability and make market entry and competition easier. But one company's definition of standards compliance may not be the same as another's. The scale of engineering work required to address idiosyncratic inconsistencies in the implementation of established

standards can be quite significant. In the context of the web, for example – though compatibility is a broader problem – the shorthand used for this is 'webcompat', or 'web compatibility'.

Differences in user experience across products as a result of insufficient compatibility can have major implications for market competitiveness.[6] Even where the inconsistencies can be addressed through additional engineering, they create friction and expense in a market environment where transactions are assumed to be low- or zero-cost. Some of this is a natural consequence of concentrated market share; when a developer can develop and test a site to work with a single browser or device or platform and know that the site will work for a healthy majority of prospective users, testing the site against others (and implementing changes as required for compatibility) represents a declining return on investment. This poses the risk of a downward spiral, for example when web developers test only on a dominant browser, which in return grows more dominant as websites work best (or only) with it.

Effective interoperability requires not only standards, but compatibility. Compatibility for the web and other markets may well prove to be an area worth further exploration, to evaluate and articulate the complex market incentives involved and the possibility of well-tailored remedies that can reduce market entry and competition costs.

Marketplaces and app stores

One of the more widely discussed dynamics of market entry in the modern internet ecosystem is in the gatekeeping role played by mobile app stores and online marketplaces. Mobile operating system providers in particular, including Google for Android and Apple for iOS, run official, sanctioned app stores, and carefully vet apps before authorising them, scanning for various legal and policy violations such as whether the app is attempting to scam or defraud users in various ways, or introduce malware or other identifiable security issues to a user's device. By default, only apps made available through official channels are allowed to be installed; varying levels of user engagement are needed to 'unlock' the user device to allow installation of software from other sources.[7] This isn't just true of mobile devices; web browsers[8] and computer operating systems[9] follow similar patterns.

In the mobile operating system context, Apple has faced criticism for many years as a consequence of its closed entry policies, though the company has also received praise for actively removing fraudulent apps from its store (Worstall 2012; Cox 2015; Gartenberg 2017). In the antitrust context, the main legal question is whether Apple's fixed 30% cut on proceeds through the app store represents an illegal use of monopoly power. In May of 2019, the US Supreme Court allowed a class action lawsuit making just such an allegation to proceed (Robertson 2018). The European company Spotify has also filed a complaint with the European Commission's competition division (Barkho 2019).

Despite this challenging history, the trend of gatekeeper control over access to applications has become the norm rather than the exception, as providers compete to become more and more trustworthy. Some level of review over third-party software, as a default practice, goes far towards reducing the prevalence of malware and fraud. The notion of interoperability in this context is thus better approached by looking at the

policies and practices set by the gatekeeper rather than the existence of a control mechanism to begin with.

In the context of web browsers, the process for developing extensions is reasonably interoperable across different browsers, with Mozilla's WebExtensions API and the Chrome Extensions API having many similarities and substantial compatibility. Operating systems are far more dissimilar technically, however, making that context likely more ripe to the potential of competition challenges.

Future US court and European Commission decisions, in the current pending cases and cases yet to come, will likely set new standards for interoperability in terms of pricing and limitations on the offering of third-party products through marketplaces and app stores.

(Mobile, web) payments

Making secure payments over the internet has come a long way since 20 years ago, when web forms without encryption facilitated the plain text network transmission of credit card numbers and other credentials. Taking this to the next level, a number of services today enable the secure payment of goods and services without entrusting the seller with credit card information, limiting the risk that can come. Payments therefore reflect a new kind of interoperability challenge, in particular for smaller sellers who must figure out how to build their transaction systems to work with different payment providers. Mobile payments, in particular, offer the potential for significant social and economic benefit in the developing world, where mobile device and network access can be more readily available than any form of traditional banking infrastructure.

The World Wide Web Consortium, or W3C, has an active working group focused specifically on web payments (Jacobs 2020). The working group aims to develop shared APIs to make it easier for merchants operating websites to exchange data with payment handlers registered with the purchasing user's web browser. Such a structure empowers internet users to adopt a number of different payment handlers and to switch across payment handlers, web browsers and merchants with relative ease – a classic illustration of interoperability as a means of reducing switching costs and thereby encouraging competition.

Mobile payment services, in contrast, generally operate through a mobile device app – colloquially a 'wallet' – that stores a user's credentials on their device and can enable payment by unlocking locally stored and secured information to authenticate individual purchase transactions. Switching across payment services or merchants is fairly easy provided each can be approved by the operator of the wallet and the device. However, switching wallets or devices requires a more active move on the part of the user.

Apple has recently introduced a digital-first credit card, encouraging users to adopt a complete vertical stack offered by Apple, including mobile device hardware and software, wallet application, credit service and physical credit card. The company has received some criticism by failing to offer a web interface to make payments on the card, requiring either an iOS device running Apple's wallet app or a phone call to a customer service representative (Nguyen 2019). This increases the lock-in effect considerably; users who choose this line of credit and card are effectively forced to use some form of Apple-provided iOS device.

The security risks associated with online payments are non-trivial, and innovation within the ecosystem to promote better security practices is certainly welcome.

However, the extent to which these innovations promote or restrict interoperability represents an orthogonal and important question.

Identity and authentication

One specific and interesting example of interoperability in practice lies in the authentication of online identity. As with mobile payments, standards have a substantial place in the current technical landscape. In particular, OAuth 2.0,[10] originally published in 2012, is well established as a standard authorisation protocol used by major online service providers, including Amazon, Facebook, Google, Microsoft and Twitter, as well as the IndieWeb community through the federated log-in protocol IndieAuth.[11] In many ways, authentication is a positive illustration of interoperability; websites can, fairly easily, incorporate OAuth-based services offered by a range of providers.

Both IndieAuth and the commercial OAuth providers are working to solve the same problem: the creation of unnecessary additional credentials, yet more usernames and passwords, and more private independent databases of credentials, creating more and more security risks for end users (particularly given the established patterns of weak and reused passwords). In this sense, centralisation offers the clear potential for security benefits.

Throughout its history, login services provided over OAuth have historically been dominated by Facebook and Google (Smith 2015). Once adopted, the lock-in effect is significant: if you use your Facebook account as the source of your identity with 20 other websites, and then choose to delete your Facebook account, you risk losing access to those 20 additional services – or at the very least, have substantial work to do to avoid losing access.

Furthermore, providing the authentication function conveys potentially valuable information to the operating platform. Necessary functionality for authentication and security of the user and their identity involves collecting and storing information about each login attempt, including, as a minimum, the location (IP address), time of access and the device and software being used. Patterns that emerge across users can reveal business intelligence that would not be derivable but for the operation of the authentication layer.

There are possible behavioural remedies that would help realise the positive security and interoperability benefits of authentication systems, while mitigating potential competitive harms. Structural separation – legally preventing shared ownership of authentication and services that use authentication – would be the most aggressive potential intervention. More limited intervention could take the form of prohibitions on tying-like contractual obligations that mandate the use of a specific authentication provider. Data transfer protections could, in theory, facilitate the necessary exchange of data while preventing the collection, storage and processing of data that could lead to competitive harm.

The competitive impact of centralisation in the operation of authentication services remains an open question, but one certainly worth further study.

Conclusion

Competition authorities around the world are evaluating their current frameworks for measuring harm and promoting competition, and are actively considering new types of

behavioural and structural remedies designed specifically for platforms. In some jurisdictions, existing antitrust law is sufficiently robust, and the authority of implementing agencies sufficiently flexible, to allow enforcement against harmful behaviours of the sort described in this paper; in others, statutory and/or administrative change is likely required. Regardless, we are entering a space where antitrust authority will be wielded more and more over time, and where the norms and balances used to differentiate between, for example, a legitimate pro-security API change and an anticompetitive act disguised as a pro-privacy move, have not yet been developed.

There are many hard, open technical questions ahead – technical both in the legal sense, of applying (and in some cases updating) existing legal standards to new market and business dynamics, and in the engineering sense, of digging into complex software and services to try to determine both the impact of, and the rationale behind, corporate practices. Competition agencies around the world will need new resources, new authorities and new processes to rise up to meet this challenge. More than that, they need new paradigms of enforcement; waiting years for complex litigation doesn't address competition challenges on internet time, and small companies facing abuse will be doomed in the market before justice or remedy can be realised.

Competition and antitrust laws are changing. Grounding future policy and legislative changes in the unique nature and varieties of gatekeeping in the digital era will help promote longer-term and more sustainable competition. Interoperability is a major factor determining the effective cost of market entry and the ongoing costs associated with growth and competition. And interoperability, as an element of the structure of a sector of the internet, determines whether a dominant market player will be able to stifle nascent competition and disruptive innovation. Through the coming changes, promoting competition and promoting interoperability will go hand in hand in the internet economy.

Notes

1. The first case in US law to find an 'essential facility', gatekeeper control of which was held to be an unlawful restraint of trade, was *United States v. Terminal R.R. Ass'n*, 224 US 383 (1912).
2. The European Commission and the governments of the United States, France, Germany, the United Kingdom, Australia, India, Israel, and likely others by the time of publication of this paper, have all undertaken processes to explore modernisation of competition policy with respect to technology and the internet.
3. 'If a user wants to switch to another product or service because they think it is better, they should be able to do so as easily as possible. This concept of allowing users to choose products and services based on choice, rather than being locked in, helps drive innovation and facilitates competition.' Data Transfer Project Overview at 3.
4. Google documents the process well at https://developers.google.com/identity/sign-in/web/sign-in.
5. For example, Slack has a thorough website for its APIs at: https://api.slack.com/.
6. Even minor delays in loading create significant economic loss, as numerous studies have shown (Einav 2019).
7. Apple mobile devices running iOS require advanced operating system kernel-level modifications through a process known as 'jailbreaking'. In Google Android devices, third party software can be installed from websites and other sources through 'sideloading', provided a user has changed their settings to allow software to be installed from 'unknown sources'. https://phandroid.com/2013/07/20/android-101-sideloading-apps/.

8. Firefox and Chrome have their add-ons (https://addons.mozilla.org/en-US/firefox/) and extensions stores (https://chrome.google.com/webstore/category/extensions) respectively.
9. Windows Apps are available in Microsoft's store (https://www.microsoft.com/en-us/store/apps/windows).
10. See OAuth 2.0 at https://oauth.net/.
11. See the IndieAuth website at https://indieweb.org/IndieAuth.

Acknowledgement

The views expressed in this article are those of the author writing in an individual capacity.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Chris Riley is the Director of Public Policy at Mozilla, working to advance the open internet through public policy analysis and advocacy, strategic planning, coalition building, and community engagement. Chris manages the global Mozilla public policy team and its active engagements in Washington, Brussels, New Delhi, and around the world. Prior to joining Mozilla, Chris worked as a programme manager at the U.S. Department of State on Internet freedom, a policy counsel with the non-profit public interest organisation Free Press, and an attorney-advisor at the Federal Communications Commission. Chris holds a Ph.D. in Computer Science from Johns Hopkins University, where he worked as a research and teaching assistant and an instructor, and a J.D. from Yale Law School, taking internships at the Electronic Frontier Foundation and the law firm Ropes & Gray. He has published scholarship on topics including innovation policy, cognitive framing, graph drawing, and distributed load balancing.

References

47 US Code § 201-02. https://www.law.cornell.edu/uscode/text/47/201.

Aspen Skiing Co. v. Aspen Highlands Skiing Corp.1985. 472 US 585.

Barkho, G. 2019. "Apple and Spotify's New Feud Signals a Complicated Future for the App Store." *The Observer*, March 15. https://observer.com/2019/03/apple-spotify-feud-app-store/.

Barrett, R. 2018. "RIP Facebook for Bridgy." *Snarfed*, August 3. https://snarfed.org/2018-08-03_rip-facebook-for-bridgy.

Bettilyon, T. E. 2017. "Network Neutrality: A History of Common Carrier Laws 1884-2018." *Medium*, December 12. https://medium.com/@TebbaVonMathenstien/network-neutrality-a-history-of-common-carrier-laws-1884-2018-2b592f22ed2e.

Bock, M. 2015. "WTF is an API? How the Internet Works Behind the Scenes". *Hackernoon*, January 20. https://hackernoon.com/apis-how-the-internet-works-behind-the-scenes-690288634c32.

Bower, J. L., and C. M. Christensen. 1995. "Disruptive Technologies: Catching the Wave." *Harvard Business Review*, January. https://hbr.org/1995/01/disruptive-technologies-catching-the-wave.

CMA (Competition & Markets Authority). 2019. *Online Platforms And Digital Advertising, Market Study Interim Report*. https://assets.publishing.service.gov.uk/media/5dfa0580ed915d0933009761/Interim_report.pdf.

Constine, J. 2018a. "Instagram Suddenly Chokes off Developers As Facebook Chases Privacy." *TechCrunch*, April 2. https://techcrunch.com/2018/04/02/instagram-api-limit/.

Constine, J. 2018b. "Facebook Shuts Down Custom Feed-sharing Prompts and 12 Other APIs." *TechCrunch*, April 24. https://techcrunch.com/2018/04/24/facebook-api-changes/.

Cox, J. 2015. "Apple Removes 300 Infected Apps from App Store" *Wired*, September 21. https://www.wired.com/2015/09/apple-removes-300-infected-apps-app-store/.

Crémer, J., Y. de Montjoye, and H. Schweitzer. 2019. *Competition Policy for The Digital Era*. Luxembourg: Publications Office of the European Union. http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

Data Transfer Project Overview. 2018. https://datatransferproject.dev/dtp-overview.pdf.

DEBA. 2016. *First Report of the Digital Economy Board of Advisors*. US Department of Commerce. https://www.ntia.doc.gov/files/ntia/publications/deba_first_year_report_dec_2016.pdf.

Digital Competition Expert Panel. 2019. *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*. London: Open Government License. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

Einav, Y. 2019. "Amazon Found Every 100 ms of Latency Cost them 1% in Sales." *Gigaspaces*, January 20. https://www.gigaspaces.com/blog/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/.

Feld, H. 2018. "Part III: Cost of Exclusion as a Proxy for Dominance in Digital Platform Regulation." *Public Knowledge*, July 19. https://www.publicknowledge.org/blog/part-iii-cost-of-exclusion-as-a-proxy-for-dominance-in-digital-platform-regulation/.

Gartenberg, C. 2017. "Apple Officially Bans Scammy Antivirus Apps from iOS App Store." *The Verge*, September 15. https://www.theverge.com/2017/9/15/16314034/apple-developer-guidelines-update-scam-anti-virus-apps-banned.

George J. Stigler Center. 2019. *Market Structure and Antitrust Subcommittee Report*. Chicago: The University of Chicago Press. https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure—report-as-of-15-may-2019.pdf.

Jacobs, I. 2020. "Web Payments Working Group Meeting in Dublin at Airbnb." *W3*, January 23. https://www.w3.org/Payments/WG/.

Lomas, N. 2015. "Meerkat Founder On Getting The Kill Call From Twitter". *TechCrunch*, May 6. https://techcrunch.com/2015/05/06/meerkat-founder-on-getting-the-kill-call-from-twitter/.

Marlinspike, M. 2016. "Reflections: The ecosystem is moving." https://signal.org/blog/the-ecosystem-is-moving/.

Microsoft Corp. v Commission of the European Communities. 2007. T-201/04.

Nguyen, N. 2019. "If You Lose Your iPhone, You Can't Pay Your Apple Card Bill on The Web." *BuzzFeed*, August 12. https://www.buzzfeednews.com/article/nicolenguyen/apple-card-with-lost-misplaced-or-stolen-iphone.

Pasquale, F. A. 2008. "Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines." Seton Hall Public Law Research Paper No. 1134159. https://ssrn.com/abstract=1134159.

Robertson, A. 2018. "What happens if Apple loses its Supreme Court App Store antitrust appeal?" *The Verge*, November 26. https://www.theverge.com/2018/6/20/17479480/supreme-court-apple-vs-pepper-antitrust-lawsuit-standing-explainer.

Search Marketing Daily. 2017. "Google To Extend AdWords API Terms Made With FTC." *MediaPost*, December 26. https://www.mediapost.com/publications/article/312183/google-to-extend-adwords-api-terms-made-with-ftc.html.

Sharma, C. 2020. "Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability." The University of Memphis Law Review (forthcoming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400980.

Smith, D. 2015. "Most People Use Facebook Or Google To Log into Other Sites And Services." *Business Insider*, January 20. https://www.businessinsider.com/most-people-use-facebook-or-google-to-log-into-other-sites-and-services-2015-1.

Sucherman, M. 2017. "Extending domain opt-out and AdWords API tools." *Google*, December 26. https://www.blog.google/outreach-initiatives/public-policy/extending-domain-opt-out-and-adwords-api-tools/.

Van der Mersch, V. 2016. "Twitter's 10 Year Struggle with Developer Relations," *Nordic APIs*, March 28. https://nordicapis.com/twitter-10-year-struggle-with-developer-relations/.

Worstall, T. 2012. "The Problem with Apple's Closed Apps Universe," *Forbes*, August 31. https://www.forbes.com/sites/timworstall/2012/08/31/the-problem-with-apples-closed-apps-universe/#16eaf627794b.