INTEROPERABILITY AS A REMEDY IN ANTITRUST CASES

BY
MITCH STOLTZ

Competition Director, Electronic Frontier Foundation.

TechREG CHRONICLE NOVEMBER 2022

Visit www.competitionpolicyinternational.com for access to these articles and more!

INTEROPERABILITY AS A REMEDY IN ANTITRUST CASES

By Mitch Stoltz

Interoperability between the products and services of different firms promotes competition by lowering switching costs. Requiring dominant firms to make their products interoperable, or reducing barriers to interoperability, are important components of competition policy for the digital age. This article makes the case for interoperability remedies in antitrust enforcement actions against Internet services. It explains the problem of "gatekeeper" firms in Internet-related markets, and describes the ways that Internet services can interoperate with one another, including through "competitive compatibility" achieved without permission from an incumbent firm. The article then lays out a spectrum of remedies that antitrust enforcers or private litigants can pursue to promote interoperability, from mandates on an incumbent firm to bans on interfering with a bona fide interoperator. Finally, the article explains how interoperability can be reconciled with the protection of users' privacy.

Scan to Stay Connected!

Scan here to subscribe to CPI's **FREE** daily newsletter.

Interoperability has always been a powerful pro-competitive tool in high-tech markets. The ability to build new products and services that are compatible with established products gives consumers more choices and helps competitors avoid entry barriers. That's why so many iconic exercises of competition policy can be seen as interoperability remedies, from the Federal Communications Commission's 1965 *Carterfone* order, to the conditions imposed on Microsoft to settle the U.S. Department of Justice's antitrust suit in 2001. In 2022, legislative proposals to address monopoly power in Internet-related markets have also included interoperability requirements, including the EU's Digital Markets Act and U.S. bills such as the ACCESS Act (H.R. 3849). But even without legislative changes, remedies in antitrust cases can be crafted to promote competition through interoperability. This article makes the case for interoperability requirements as antitrust remedies: why they should be included, how to craft them, and how to reconcile interoperability with user privacy.

01
THE LANDSCAPE OF GATEKEEPER PLATFORMS

There is widespread concern about increases in market concentration, the presence of monopoly power, and greater centralization of services in Internet-related markets. Policymakers and opinion leaders have placed particular emphasis on persistent market power among "gatekeeper platforms" — Internet services that play an outsized role in the digital lives of U.S. consumers. These include the various online offerings of Meta Platforms (formerly Facebook), Google, Apple, Amazon, and perhaps Microsoft. Other firms that control significant market share in particular Internet-related markets such as online gaming may also be gatekeepers, or could become so.

Although the core services offered by each of these companies differs, the policy concerns they raise are similar: each one effectively controls access to a large share of customers for other Internet apps and services, including nearly all businesses that could potentially compete with the giants in their core services. For example, Meta and Google together control about half of the market for online advertising, which is a primary revenue source for online publishing. Ongoing antitrust suits accuse Meta of having a dominant position in social networking. Amazon and Microsoft provide a dominant share of the cloud services used by businesses of all sorts.

Many of the gatekeeper platforms have wielded market power to the detriment of consumers. For example, Facebook made repeated public commitments to maintain users' privacy in particular ways, and repeatedly reneged on those commitments. Facebook's conduct suggests that as its market share grew and rivals like MySpace and Google Plus exited the market, the company was able to make its service less privacy-protective without losing users — evidence of monopoly power and of consumer harm.

Recognizing these harms, federal and state antitrust enforcers, along with private plaintiffs, have brought numerous antitrust suits against the gatekeeper platforms over the past several years. In Europe, significant antitrust enforcement against these companies by the European Commission and state enforcers began several years earlier and remains strong.

The remedies sought in legal actions to date have primarily been monetary recovery and fines. Although fines have increased over time, they may still be inadequate to cause significant changes to the gatekeepers' business practices. The recent European Commission fine of $4.12 billion against Google for the company's practices to exclude competing search engines and browsers was just 1.5 percent of the company's 2021 global revenues. Compared to the potential value of maintaining a firm's position as a gatekeeper to consumers, even multi-billion-dollar fines may simply become a cost of doing business.

Injunctions or negotiated settlements designed to promote interoperability between the products of a firm with market power and other firms' products are an alternative remedy that enforcers can employ.

02
TYPES OF INTEROPERABILITY

Pro-competitive interoperability between digital products and services takes different forms in practice. At its most comprehensive, the services of an incumbent and a challenger can share data, and invoke each other's functionality, through their common use of open standards created by an independent standards body. Email is an example of this, along with most of the protocols that underlie the basic functions of the Internet, such as the Hypertext Transfer Protocol ("HTTP").

Incumbent firms also invite makers of complimentary goods and services to interoperate by giving them access to proprietary specifications (often called Application Programming Interfaces or APIs) controlled by the incumbent. Makers of mobile operating systems, such as Apple's iOS and

© 2022 Competition Policy International All Rights Reserved

Google's Android, have enabled markets for third-party mobile apps by exposing their APIs to developers.

Interoperability frequently happens without significant coordination between an incumbent firm and a challenger. Many entrepreneurs build new products or services to be compatible with existing ones by reverse-engineering the existing product and deriving the technical requirements for interoperability, often without permission from the incumbent. Many important innovations have come from such "competitive compatibility." For example, Cydia was a long-running alternative app store for Apple devices that featured software programs that were not available from Apple or Apple-authorized developers. Using Cydia, and the apps it supplied, required "jailbreaking" an Apple device — defeating some of its security measures to permit loading software not authorized by Apple. Many features that today are incorporated into iOS itself began as apps or modifications available on Cydia, including copy/paste functions, interactive alerts, and alternative keyboards.

One important form of competitive compatibility is the creation of alternative user-side apps for interacting with an incumbent platform. For example, independent developers have created alternative client programs for users of Facebook, Instagram, Slack, and various instant messaging platforms. Some of these are complete drop-in replacements for an incumbent platform's own app, while some are browser plug-ins or customized browsers. Alternative clients can allow users to customize their experience of an incumbent platform through custom ordering and filtering of posts, blocking advertisements, hiding "likes" and other social feedback, or combining data from multiple platforms. Sometimes this is achieved entirely within an alternative app or browser running on the end user's device, and sometimes it may involve use of third-party servers or cloud computing resources.

03
PRO-COMPETITIVE EFFECTS OF INTEROPERABILITY

In Internet-related markets, probably the most important effect of interoperability is its potential to reduce users' cost of switching between platforms. Taking Facebook as an example, many users continue to spend significant time on the platform not because its features and design best suit their needs, but because it's where their social connections reside. If Facebook is the place a user has to go to see messages or posts from her friends, announcements from the businesses or clubs they frequent, photos of their family, and so on, then she will spend more time on Facebook than on potential rival apps, even if an alternative might be more privacy-protective or have curation and editorial practices that she prefers. This tendency gives Facebook an advantage deriving from the size of its user base rather than the quality of its offerings, and engenders an anticompetitive market failure.

Now imagine that a user can leave Facebook for an alternative social network — call it User Republic — that interoperates with Facebook. She can view posts and news stories published on Facebook, but those posts are prioritized and filtered according to the algorithmic policies of User Republic rather than Facebook. Private messages sent on one service can reach users on the other, if users consent to be reached in that way. The user now has a feasible alternative that avoids many of the most-criticized features of an incumbent like Facebook, such as poor privacy practices and an editorial model that promotes false or divisive content. This is a "federated" model of interoperability.

Some of these benefits can also be realized with alternative client apps, sometimes called "delegability." As described above, an alternative app could interact with the Facebook servers on behalf of a user in place of Facebook's own app and website. This could allow for better user control over the personal data sent to Facebook's servers. It can also allow for reordering or filtering data feeds, and for combining messages and posts from different platforms within a single interface. Although alternative apps don't provide a way for users to leave an incumbent platform entirely, as a federated model could, the app approach can still put competitive pressure on the incumbent to improve its service vis-a-vis other services that can be accessed through the same app.

These forms of interoperability can lead to lower switching costs for users. If users can more easily leave an incumbent platform, the incumbent will face market pressure to improve its services, including better safeguarding users' privacy. If competing services offer compelling alternatives to the incumbents' content moderation and curation, then the incumbents will be driven to improve their own. Security, too, could become a source of competitive pressure: if switching to alternative platforms is easy, we can expect that well-publicized security breaches or other betrayals of users' trust will lead to larger, sustained movement of users to other services.

Intensifying this dynamic, network effects may amplify the impact of users leaving a platform. Migration of users may cause a market to "tip" to another leader, creating an accelerating trend. This occurred between 2009 and 2011, when users began to move from then-leading social network MySpace to Facebook. The shift began, in part, because of dissatisfaction with MySpace's privacy practices, and Facebook's offer of better privacy. Once begun, the shift became self-sustaining, until MySpace faded into ir-

© 2022 Competition Policy International All Rights Reserved

relevancy. Attempting to avoid this dynamic will place even greater pressure on incumbent platforms to move towards better privacy, security, and user empowerment.

04
POSSIBLE APPROACHES TO COMPETITION REMEDIES

In antitrust and consumer protection cases involving online platforms with market power, enforcers can propose injunctive or negotiated remedies that promote these forms of interoperability. These remedies can include affirmative *obligations* on an incumbent firm to allow third parties to interoperate, *prohibitions* on the use of various legal or technological measures to prevent interoperability, or some combination of these.

Affirmative obligations can be stated broadly in terms of a desired outcome — for example, ordering an incumbent platform to achieve interoperability for specific applications or features (such as the ability to send and receive private messages) with other firms that request it. Stating a required outcome rather than a means of achieving it keeps the court or enforcement agency out of the technical details, and may create a fix that is more resilient in the face of technological change. It may, though, require monitoring and revision if the set of features that must be interoperable to meet user demand changes — for example, if users shift from text-based private messaging to video messages, an interoperability requirement for private messaging might have to be expanded to include video.

This is largely the approach taken by the Digital Markets Act ("DMA"), passed this year by the European Union. The DMA requires that covered companies make their messaging services — likely including Facebook Messenger, Instagram direct messaging, WhatsApp, and Apple's iMessage, interoperable with other messaging services on request. The regulation requires that text messaging be interoperable on request within the coming year and video within two years.

This approach probably requires a significant amount of monitoring by enforcement agencies or private litigants, and additional adversarial proceedings when circumstances change, or parties disagree about whether the requirements have been met. It may also require ongoing investigative powers (such as the right to review documents) to test the parties' claims.

A related but narrower approach is to require the incumbent to interoperate with third parties through an existing technical standard or protocol, either one created by a formal standards organization or through a private collaboration. Requiring the use of an existing standard can make compliance easier to ascertain and limit the scope of future enforcement conflicts. But this approach means that the set of interoperable features may become obsolete and less relevant to users. If that happens, the requirement would fail to promote user mobility and drive competition.

The other approach to an interoperability remedy is one stated in terms of a prohibition: an incumbent firm can be forbidden to interfere with or block interoperators through various legal and technical means. When challengers engage in competitive compatibility — building compatible products and services through reverse engineering — incumbents often respond with legal threats. These threats can be grounded in various legal theories: patent, copyright, laws like the federal Computer Fraud and Abuse Act, and business tort theories such as tortious interference with contractual relations. An injunction against asserting these types of claims against bona fide interoperators may be enough to let adversarial interoperability flourish, for products and services that are reasonably susceptible to reverse engineering. In circumstances where meaningful compatibility can't be done without proprietary information from the incumbent, such as cryptographic keys, an additional requirement to share such information might be needed.

Either type of interoperability remedy — positive requirements or bans on interfering with competitive compatibility — can also be imposed to protect alternative client apps that access an online service. This is sometimes called *delegability* because it protects users' ability to delegate their interactions with a platform to a third-party intermediary.

05
SQUARING INTEROPERABILITY WITH PRIVACY

Interoperability in Internet-related markets can raise privacy risks. A competitor who has access to users' data and communications through interoperating with an established platform may misuse that data carelessly or maliciously. An incumbent platform can claim to protect

© 2022 Competition Policy International All Rights Reserved

its customers' privacy by refusing to interoperate with third-party companies, or by limiting that interoperability. After Facebook faced the uproar regarding Cambridge Analytica's misuse of data collected on its platform, its primary response was to shut down the "Platform API" used by third-party apps to access Facebook user data, while continuing to collect the same data for its own use.

Protecting privacy, though, doesn't justify a complete refusal to interoperate. Giant incumbent platforms do have a market incentive to protect their users, but that incentive is frequently overcome by other commercial interests. Apple frequently uses its efforts to protect user privacy as a selling point, but the company also prevents users from taking steps to enhance their own privacy when doing so conflicts with Apple's interests. For example, Apple bans virtual private network (VPN) apps and other privacy-enhancing tools from its app store for users in China.

For purposes of an interoperability remedy, the most effective solution is comprehensive consumer privacy legislation. The European General Data Privacy Regulation ("GDPR") and the California Consumer Privacy Act are attempts at this, although none has yet been passed at the federal level in the U.S. A "baseline" guarantee of consumer privacy that is applicable to all firms in a market would remove the biggest policy obstacle to interoperability.

That said, interoperability remedies don't need to wait on comprehensive privacy regulation. They can be designed to allow the incumbent platform to limit or even refuse interoperability with a specific app or service when the platform can identify a concrete privacy risk, such as evidence that an app or service is misusing data obtained through its link with the incumbent platform. In emergency circumstances, such as the discovery of a serious security vulnerability, the platform should be able to switch off the interfaces used for interoperability quickly and without prior approval from the court or antitrust enforcer, but the platform should be required to justify their actions after the fact, and to tailor a cut-off as narrowly as possible to the affected app. Outside of these circumstances, allowing complimentary products and services to interoperate with the incumbent should be the norm, even if those products and services are also competitors.

The Federal Communications Commission's 1968 *Carterfone* order illustrates how to craft a rule that harmonizes security (and privacy) with the procompetitive effects of interoperability. At the height of its monopoly control over telecommunications, AT&T argued that reliable operation of the telephone network required their "absolute control over the quality, installation, and maintenance of all parts of the system," and therefore banned all third-party devices from its network. To "divide the responsibility for assuring that each part of the system is able to function effectively," argued AT&T, would inevitably create a poorer experience for customers. When Carterfone, a competing maker of specialized telephone equipment, asked to be allowed to connect to the phone network, the FCC rejected AT&T's broad presumption that any interoperability would create inherent risks to the operation of the network. AT&T could only refuse to interoperate, the FCC ruled, in specific cases where it could show actual harm.

Requirements for interoperability — or requiring a firm not to stand in the way of it — are important tools that should be in every antitrust enforcer's toolbox. Crafted carefully, they can unlock competition to better serve technology users.

That said, interoperability remedies don't need to wait on comprehensive privacy regulation

© 2022 Competition Policy International All Rights Reserved

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL

© 2022 Competition Policy International All Rights Reserved