

# Appendix 2: Key Features of the Digital Platform Agency

*The behavioral differences between traditional industries with relatively stable technology and new digital businesses with rapidly evolving capabilities demand a new approach to public oversight. Attempts to repurpose existing federal agencies perpetuates old procedures, practices and precedents developed for the realities of a different era. The solution must be more than attempting to clone industrial era regulatory tools to meet digital era needs.*

## **Regulatory Success In A Digital Environment**

We too often forget that the mid-19th and early 20th centuries were also times of unprecedented technology-driven change that upended social and economic norms.

Creating a new agency is well in line with how the government has responded to technological advances in the past. The advent of railroads in the mid-19th century brought forth issues of behavioral abuse in a novel, yet vital, industry. In response, the Interstate Commerce Commission (ICC) was created in 1887. In a similar vein, the advent of radio technology quickly triggered a federal role, culminating in the 1934 creation of the FCC.

Digital platforms are the railroads and radio of the 21st century, occupying a similarly important position in modern society. Just as railroads opened up the West, today's search engines and social networks do the same for the Internet, permitting its potential to be more fully realized in terms of improvements in existing services and the creation of entirely new ones.

We too often forget that the mid-19th and early 20th centuries were also times of unprecedented technology-driven change that upended social and economic norms. Policymakers of that era had to step up to balance the power of new technology-based enterprises with the public interest. While we may look back on that era as simpler times, to those involved the changes they were called upon to deal with were as revolutionary, disruptive, and potentially harmful as today's transformations.<sup>63</sup>

The regulatory structures developed to deal with the new realities of the industrial era reflected the characteristics of the dominant companies of the era—characteristics that have been upended by digital technology. Twenty-first century technology and market realities require a new regulatory structure of nimble oversight tools unpossessed by the agencies that still today oversee industrial markets.

In the new times of the digital era, there is a need for new solutions to the oversight of companies with significant market power and societal effect.

## **Digital Platforms are Different**

Digital platforms have grown to dominate key portions of the economy in ways that are significantly different from their industrial predecessors. By galvanizing

Twenty-first century technology and market realities require a new regulatory structure of nimble oversight tools unpossessed by the agencies that still today oversee industrial markets.

the power of network effects, economies of scope and scale, and massive amounts of data previously unachievable due to the inability to collect and exploit it, a few dominant firms rule over online search, social networking, e-commerce and the digital advertising market—activities fueled by the companies’ dominant data power.

This possibility was identified by FTC Commissioner Pamela Jones Harbour in her extensive Dissenting Statement in Google’s 2007 acquisition of DoubleClick:

*“[M]arrying the [Google and DoubleClick] datasets raises long-term competition questions that beg further inquiry.*

- *In a post-merger online advertising market driven by the value of behavioral targeting, will Google/DoubleClick face meaningful competition?*
- *Will any other firm be able to amass a dataset of the same scope and size?*
- *Will any other company be able to overcome network effects and offer an equally focused level of behavioral targeting?*
- *If advertisers and publishers have to channel their online advertising through Google/DoubleClick in order to access the best dataset that supports targeted advertising, will any other firms have the ability or incentive to compete meaningfully in this market?”<sup>64</sup>*

The ability to join advertisers, sellers of products, and content creators with billions of consumers relies on the vast amount of data collected and then hoarded by the companies selling those connections. With such data as the essential digital asset, its control creates a virtually insurmountable hurdle to competition. Neither antitrust nor traditional regulatory tools are capable of moving nimbly or quickly enough, let alone reliably enough, to address immediate impediments to competition and fair dealing that result from the power of dominant digital platforms.

Competing in the digital marketplace requires access to the raw material of data. The dominant digital companies have achieved their position through control over massive amounts of data. Companies seeking to compete against one of the dominant platforms confront the reality that advertisers pay for the demographic granu-

<sup>63</sup> For example, Professor, later Chief Judge, Arterburn raised this question as new regulatory possibilities were surfacing in 1927:

A field of law that is enclosing within itself vast portions of old law, at an unusually rapid rate today, is that which concerns businesses affected with a public interest. The exact direction which this development shall take, accelerated by the immense pressure brought by our industrial structures of this day, is open to wide and interesting speculation. Whether it will eventually include all businesses within its grip, like a giant octopus pressing its unwelcome hold, silently and unconsciously upon one class of business at a time, or whether it shall soon be caught and held within bounds by definite rules soundly worked out, is worth considering. We have the view presented of a bureaucratic government regulating every phase of human activity. Whether our government is progressing or retrogressing at this time, we should know. Are we reverting to the paternalism of the thirteenth century, or the laissez faire policy and extreme individualism of the seventeenth and eighteenth centuries? Or is it a middle course we are steering?

Arterburn, *supra* note 16.

<sup>64</sup> In the matter of Google/DoubleClick F.T.C. File No. 071-0170, Dissenting Statement of Commissioner Pamela Jones Harbour, 8 (Dec. 20, 2007), [https://www.ftc.gov/sites/default/files/documents/public\\_statements/statement-matter-google/doubleclick/071220harbour\\_0.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/statement-matter-google/doubleclick/071220harbour_0.pdf).

Neither antitrust nor traditional regulatory tools are capable of moving nimbly or quickly enough, let alone reliably enough, to address immediate impediments to competition and fair dealing that result from the power of dominant digital platforms.

larity made possible by massive amounts of data on a massive number of individuals.

When Facebook began in 2004, the leading social media company was Myspace, owned in part by Rupert Murdoch’s News Corp. In those days, data aggregation and exploitation had yet to achieve its subsequent dominance. As a result, Facebook was able to displace Myspace through old-fashioned “my product is better” competition. Today, if a new “better than Facebook” product were to come along, the services it could sell to advertisers—and thus its revenue potential—would be sorely limited because of its limited reach as compared to the vast trove of user and related data Facebook has collected and hoarded. As Professor Fiona Scott Morton and antitrust attorney David Dinielli pointed out in a recent paper:

*Facebook harvests vast stores of data based on users’ interactions with its own platform as well as users’ activities off Facebook that Facebook tracks such as location and purchases. Assuming that a new entrant would also be ad supported, no de novo entrant would have access to anywhere near the volume or quality of data that Facebook can access until it reaches the same level of scale (which is difficult because of network effects etc.) and privacy intrusiveness.<sup>65</sup>*

What is needed is an agency that can quickly adopt and enforce broad-based rules, then apply them both ex post and ex ante to quickly spot and rectify harmful digital market practices. Remedies ranging from access to data, to nondiscriminatory algorithms, to open network interfaces, to interoperability require first, a statute applying common law-derived principles to the digital market, and second a substantial level of technical expertise. The goal of such oversight should be the development and application of accepted industry standards to build workable public interest guardrails against abuse. No existing agency has this skill or agility today.

### **Digital Oversight Must be Different**

Agencies such as the Federal Trade Commission (FTC) have been suggested for this oversight. That the FTC is populated by dedicated professionals, there is no doubt. Similarly, there can be no doubt that Congress has for many years constrained the agency’s appropriation and jurisdiction when the FTC tried to be proactive.<sup>66</sup> Given its broad responsibilities over an expansive collection of traditional marketplace activities, including its continuing enforcement of antitrust law, the FTC’s resources are already spread thin. The new economy requires a “digital-all-the-time” agency, not the sharing of resources between the industrial and digital economies. This focused oversight necessitates not only a specialized form of regulation, but also a new approach to the development of such policies as outlined in Appendix Three.

<sup>65</sup> FIONA SCOTT MORTON & DAVID DINIELLI, ROADMAP FOR AN ANTITRUST CASE AGAINST FACEBOOK, 18, Omidyar Network (Jun. 2020), <https://www.omidyar.com/sites/default/files/Roadmap%20for%20an%20Antitrust%20Case%20Against%20Facebook.pdf>.

<sup>66</sup> See Harold Feld, *How Not To Train Your Agency, Or Why The FTC Is Toothless*, TALES OF THE SAUSAGE FACTORY (Mar. 15, 2019), <https://wetmachine.com/tales-of-the-sausage-factory/how-not-to-train-your-agency-or-why-the-ftc-is-toothless/>. Feld argues that the FTC was punished for its enforcement through the cabining of its authority in the FTC Improvement Act of 1994.

Because antitrust law does not impose the traditional common law duty of care and only sparingly adopts the duty to deal that many federal agencies apply to other commercial sectors, Congress must empower a new agency to do so for digital firms.

Such a new agency would augment, not replace, the agencies responsible for enforcing antitrust law. The job of the Digital Platform Agency (DPA) would be the protection of both consumers and competition through the application of nimble regulatory tools and speedy dispute resolution consistent with the dynamic nature of digital markets. Because antitrust law does not impose the traditional common law duty of care and only sparingly adopts the duty to deal that many federal agencies apply to other commercial sectors, Congress must empower a new agency to do so for digital firms.

Such digital oversight should be different from traditional industrial oversight in two ways. First, the responsibility of the new agency should be to make judgment calls about ever-changing marketplace activities based upon congressionally determined behavioral principles. Second, in exercising such responsibility the new agency will utilize behavioral codes developed by an industry/public expert group whose actions are supervised and approved by the agency.

Scholars with extensive backgrounds in both antitrust and regulation have suggested the need for a similar approach to digital market accountability. In a recent article, Professors Howard Shelanski and Bill Rogerson first identify the weaknesses of antitrust for addressing digital platform concerns and then suggest an approach like the DPA:

*We nonetheless find three main reasons why, despite the challenges in getting regulation right, limited regulation might have advantages over traditional antitrust adjudication in the context of large-scale industries with network effects. First, . . . the adjudicative model for antitrust enforcement and doctrinal development has met with well-founded criticism. . . . Second, traditional antitrust remedies might not effectively address the competitive challenges of digital platform markets. . . . Third, . . . conduct that courts ordinarily judge under antitrust law’s general rule of reason might have different presumptive effects and therefore be better governed by a more specific set of standards in digital platform industries. An expert agency might be particularly suited to determine when ‘outer-boundary’ theories of harm that courts rightly disfavor for general applications—theories of harm like predation, refusals-to-deal, or acquisition of nascent competitors—should apply in specific contexts.<sup>67</sup>*

Shelanski and Rogerson go on to identify specific telecommunications rules as successful forms of regulation pertinent to digital platforms: “Regulations designed to increase competition by reducing switching costs have had notable success in the telecommunications industry. In particular, in 2003 the FCC introduced regulations that allowed mobile telephone subscribers to take their telephone number with them when they switched mobile telephone providers, thereby significantly reducing the costs of switching providers. This is widely thought to have increased levels of competition in this mobile telephony.”<sup>68</sup> They then conclude:

*traditional antitrust adjudication is unlikely to remedy the problems of platform markets, or to do so in a blunt way that does not apply technical expertise to ensure that remedies are effective and beneficial. In this article, we identify forms of regu-*

<sup>67</sup> William P. Rogerson & Howard Shelanski, *Antitrust Enforcement, Regulation and Digital Platforms*, 6–7 (Apr. 18, 2020) (unpublished manuscript, on file with author) (forthcoming in U. PA. L. REV.)

It falls to Congress to fully embrace the reality of the digital era with the first designed-for-digital federal agency.

*lation we think could, in the specific context of dominant digital platforms, improve on the adjudicative model of antitrust enforcement while avoiding the most significant costs and burdens of traditional public utility regulation. Through limited and non-discriminatory access and interconnection, digital platforms could continue to innovate, compete, and provide network benefits to their users while at the same time ensuring that actual and potential competitors can enter, gain traction, and expand their appeal to consumers.<sup>69</sup>*

The U.K.’s expert antitrust agency, the Competition & Market Authority (CMA) has come to a similar conclusion regarding oversight of digital platforms. In its recent Market Study on the digital advertising market, the CMA concluded that “there is an urgent need to develop a new pro-competition regulatory regime for online platforms.” The CMA proposes a “regulatory regime with strong ex ante rules which can be enforced rapidly and updated as required.” This includes “A binding code of conduct with strong powers to sanction non-compliance.”<sup>70</sup> The CMA goes on to say:

- “The code would govern the behavior of online platforms with strategic market status. This would include both Google and Facebook.
- The code would be structured around the high-level objectives of: ‘fair trading’; ‘open choices’; and ‘trust and transparency’.
- A Digital Markets Unit (DMA) would be empowered to enforce the code, penalizing firms for non-compliance where appropriate and developing the code over time, ensuring concerns can be dealt with swiftly.

The DMA should also have powers to introduce ‘pro-competitive interventions’ to tackle sources of market power and increase competition, including powers to provide access to data, to support consumer choice and to order the structural or functional separation of platforms where necessary.”<sup>71</sup>

### **Statutory Underpinnings**

It falls to Congress to fully embrace the reality of the digital era with the first designed-for-digital federal agency. There are three core concepts such legislation must address:

- Oversight of digital platform market activity on the basis of risk management rather than micromanagement; this means targeted remedies focused on market outcomes and thereby avoids rigid utility-style regulation,
- Reaffirmation of common law principles of a duty of care and a duty to deal as the underpinning of DPA authority, and
- Delivery of these results via an agency that works with the platform companies to develop enforceable behavioral codes while retaining the authority to act independently should that become necessary.

<sup>68</sup> *Id.* at 48.

<sup>69</sup> *Id.* at 64.

<sup>70</sup> *CMA Final Report*, *supra* note 14.

<sup>71</sup> *Id.* at 322.

In the absence of federal policy, the dominant digital companies have assumed the role of a pseudo-government to make the rules for the digital marketplace.

What follows describes the underlying concepts of the statutory framework needed to meet the digital market challenge, as well as examples of where and why the new agency should be involved.

**Risk Management, not Utility Regulation:** rather than monitor costs, prices, or prohibit specific behaviors as was a common practice for industrial era regulation, the digital marketplace requires a more flexible set of standards informed by common law-derived norms that demand specific market outcomes. A new agency must manage risk to prioritize competitive market outcomes and consumer protection as precisely as possible to preclude or ameliorate risky behavior most harmful to competition and consumers. For the DPA this means that the process of risk management requires a focus on market outcomes instead of utility-style regulatory mandates.

### **Statutory Directive – Restoring Common Law Principles to Digital Activities**

In the absence of federal policy, the dominant digital companies have assumed the role of a pseudo-government to make the rules for the digital marketplace. In the process, basic concepts that have been redefined and applied to economic activity for centuries have been conveniently ignored. The authorizing legislation for the new digital agency should be based around the agency's application of such common law concepts to digital activities.

The duty of care establishes that it is the responsibility of a purveyor of goods or services to anticipate and mitigate the harmful effects that might result from those activities. The contemporary concepts of negligence, for instance, are derivative of the duty of care, as it has evolved over the centuries. When the railroad spread and amplified the industrial revolution, for instance, application of the duty of care principle determined that the railroad companies had a legal duty to anticipate and mitigate that the hot cinders spewing from smokestacks could set fire to the barns and hayricks their locomotives passed. Similarly, from the time of the earliest automobiles, courts imposed a duty of care on car manufacturers even for faulty parts although the parts were made by a third party. As the dominant digital companies drive the information revolution, they, too, have a responsibility for curbing the negative consequences of their actions. This includes prudent handling practices and treatment of consumer and commercial data.

The duty to deal is another common law-derived concept that must find root in the digital economy. When a service is essential or critical owing especially to its monopoly characteristics, there is a duty to provide non-discriminatory access to that service.<sup>72</sup> The Pacific Telegraph Act of 1860 established such a policy for the essential information service of that era by mandating non-discriminatory access. The internet is the essential service of this era and those companies that collect and store its critical asset—data—should have a commensurate duty to deal, to not monopolize that asset. This should include, for instance, nondiscriminatory access through interoperable interfaces, free flow of data across services providers, and limits on preferencing dominant platforms over competitors.

The Agency should be directed to promote competition and protect consumers with a specific set of tools built around the duty of care and duty to deal. Such

The Agency should be directed to promote competition and protect consumers with a specific set of tools built around the duty of care and duty to deal.

oversight would extend across all digital platform activities including social media and e-commerce, but (as discussed below) applied in a manner so as to avoid unnecessarily burdening smaller companies. This is not to interfere with the jurisdiction of existing federal agencies (e.g., oversight of an e-commerce company's prohibition of tainted goods or false advertising).

### **Who is Subject to These Duties?**

The Agency's tools related to establishing the duty of care must be targeted towards critical values not otherwise protected such as privacy and the security of personal information, and the duty to deal should be limited to platforms deemed systemically important to society due to their economic dominance or essential nature.

The Agency will need to determine what companies are systemically important in their social and economic impact. This is not a new role for government. The Dodd-Frank Act, which focused on preventing financial collapse, described systemically important as involving companies that "need not be massive," but are "essential to the workings of the financial system." The key feature the Act highlights is that systemically important companies' "failure would trigger a cascade effect that could cripple the entire system they inhabit."<sup>73</sup> The DPA should develop criteria for digital market companies that reflect this same degree of importance to the workings of digital markets, as Dodd-Frank did for the financial system.

### **An Example of Systemically Important Power: Bottleneck Power**

The Agency should also determine which companies are systemically important as a result of their dominance or bottleneck power. For example, the DPA must assess whether network effects, economies of scale, economies of scope, power over data and similar factors have given certain companies excessive economic or social power, most often reflected by having a dominant position—bottleneck or gatekeeper control—over a key aspect of the digital market.

The Stigler Report defines bottleneck power this way:

*"Bottleneck power" describes a situation where consumers primarily single-home*

<sup>72</sup> As noted, this legal proposition originated many centuries ago and has been deployed continuously as economic circumstances have dictated. See Arterburn, *supra* note 16, at 420–21 (citations omitted):

Businesses, it is true, had certain peculiar duties placed upon them, such as the duty to serve all who applied; but this was because of the peculiar economic conditions of the time, it is believed. The reason for these duties being placed upon a business, was not because it was "public" but because it was more important to the public at the particular time. All trades in time of distress or economic paralysis were affected with a very high degree of public interest. The duty to serve, and not the duty to use care, in such times, was the distinguishing feature of the public interest of the trade or business. Those upon whom the duty to serve is placed may vary with economic conditions, but not those upon whom the duty to use care is placed.

<sup>73</sup> Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 929-Z, 124 Stat. 1376.

The consumer protection and competition promotion functions of the DPA are designed to enhance and not replace what other existing Federal agencies do.

*and rely upon a single service provider (a “bottleneck”), which makes obtaining access to those consumers for the relevant activity by other service providers prohibitively costly.<sup>74</sup>*

Similarly, the Furman Report defines gatekeeper power:

*[O]ne, or in some cases two firms in certain digital markets have a high degree of control and influence over the relationship between buyers and sellers, or over access by advertisers to potential buyers. As these markets are frequently important routes to market, or gateways for other firms, such bottlenecks are then able to act as a gatekeeper between businesses and their prospective customers.<sup>75</sup>*

Firms may benefit from bottleneck or gatekeeper power due to economic forces that impede entry and foreclose large swaths of the market from competition. Both the Stigler and Furman Reports note the significant impact that high consumer switching costs can have on the operation of a competitive market. Psychologists and economists have studied how the inertia of default choices<sup>76</sup> pushes users towards single-homing—i.e., locking into a single platform in pursuit of convenience. But it is not just convenience that locks consumers to a provider. Often the product itself is designed with technological barriers to switching precisely for the purpose of preventing consumer choice. Similarly, it is sometimes argued that it is “technically necessary” to have tying between two products. Such practices should be remitted to specialists if it involves significant social consequence. Digital businesses that have this incentive and ability to develop and preserve a single-homing environment should be a specific focus of the DPA because of their bottleneck or gatekeeper power.

### **Relationship to Other Agencies and Laws**

The consumer protection and competition promotion functions of the DPA are designed to enhance and not replace what other existing Federal agencies do regarding digital technology in their jurisdiction. Federal agencies as diverse as the National Highway Traffic Administration (NHTSA) and Food and Drug Administration (FDA) deal with the impact of digital technologies in their areas of focus. Nothing in the authorizing statute for the DPA should in any way limit or affect existing federal statutes. Most importantly, the DPA should not duplicate the activities of the principal antitrust agencies but instead complement those activities.

The Agency should be expected to provide the federal antitrust agencies with advice regarding transactions involving systemically significant firms and provide advice regarding any antitrust investigations or prosecutions whenever the antitrust agencies seek such input. Similarly, the DPA should be expected to provide advice to the FTC’s investigations or prosecutions of digital platforms pursuant to the FTC’s deceptiveness and unfairness jurisdiction. Finally, the Agency would

<sup>74</sup> STIGLER ANTITRUST REPORT, *supra* note 12, at 84.

<sup>75</sup> FURMAN UK REPORT, *supra* note 22, at 41.

<sup>76</sup> See, e.g., DANIEL KAHNEMAN, THINKING FAST AND SLOW, Farrar, Straus and Giroux (2011); RICHARD THALER AND CASS SUNSTEIN, NUDGE, Yale University Press (2008).; and MICHAEL LEWIS, THE UNDOING PROJECT, W.W. Norton (2016).



Interoperability  
is the heart  
and soul of  
the internet.

act as the monitor of systematically important firms subject to judicial decrees involving such firms.

### **Examples Of Agency Interventions**

#### *Interoperability*

Interoperability is the heart and soul of the internet. Originally called “internet-working,” the internet is nothing more than a standard way to interconnect disparate networks. That the platform companies take advantage of such interconnection to deliver their products but then deny interconnection to their service is a perversion of the internet itself and an affront to the public interest.

Factors that encourage reliance on one provider, referred to as single-homing, may be inherent to the economics and technology, or they may be policy decisions made by the incumbent platform. A recent analysis summarized much of the accumulated learning on the subject. “[E]ntities with disproportionately large amounts of information have relatively little to gain and much to lose from sharing the information that they collect. Indeed, by refusing to share information data with their smaller rivals, large entities may be able to eliminate these rivals as competitors and instead turn them into customers.”<sup>77</sup> Thus, a dominant platform’s policy not to provide interoperability between its services and those of competitors should be viewed skeptically. Such corporate decisions are reflected, for instance, in technical standards and contracts, including methods for denying critical market data to users and competitors. Competitors may find their own way to provide interoperability without permission, sometimes called “adversarial interoperability,” and incumbents may affirmatively choose to block this when they discover it.

In a world where, for instance, access to a social network’s user base can make or break a small company’s picture sharing or messaging service, it is critical to separate reasonable security or privacy interconnection specifications from unfair impediments to competition. The same is true for connecting advertisers and content providers through real-time bidding and lightning-speed auctions on digital advertising exchanges.

Government oversight of interconnection responsibilities is not new. Even before the internet, the FCC struggled for decades with interconnection between large and small telephone companies, between long distance and local telephone companies, or between telephone common carriers and private network service providers.

As Dr. Stanley Besen noted:

*It is useful to begin the discussion of compulsory data sharing by exploring an analogous situation drawn from another context: carrier interconnection in the telecommunications industry. As [Professor Eli] Noam has noted:*

*The historic experience with interconnection around the world shows that interconnection is not made available freely by an incumbent to its competitors. Nor is the claim to interconnection as a right given up voluntarily by new entrants once competition emerges.... Often, the terms of interconnection are left nominally or*

<sup>77</sup> Stanley M. Besen, *Competition, Privacy, and Big Data*, 28 Cath. U. J. L. & TECH 63, 70 (2020) (citations omitted).

Government oversight of interconnection responsibilities is not new.

*initially to the parties' negotiation. Yet regulatory intervention is frequent where there is an asymmetry in bargaining strength and in the urgency for interconnection, which is usually the case. Even where formal regulatory intervention does not take place, the negotiations are shaped by the expectations of what the regulator's decisions would be. Those decisions, in turn, depend on fundamental policy priorities. As a matter of empirical fact, interconnection is regulated everywhere where competitive telecommunications exist.*

The point here is that, just as interconnecting with their smaller competitors is likely to erode the competitive advantage of large telecommunications carriers, so that those carriers are unlikely to be willing to interconnect unless compelled to do so by regulators, firms with large amounts of data are also likely to be unwilling to share their data with their smaller competitors. ... [As] Professors [Daniel] Rubinfeld and [Michal] Gal argue that “[i]f the source of the barriers [to data sharing] is inherently structural, and sharing the data is socially beneficial, a regulatory solution may be appropriate, perhaps by requirements that the data be made widely available at a reasonable and non-discriminatory cost....

*As the experience in mandating interconnection in telecommunications makes clear, mandating data sharing is unlikely to be straightforward. Although the necessary cooperation among telecommunications firms is limited to completing calls that originate on the networks of other operators, disputes can nevertheless arise regarding, among other things: (1) the locations at which interconnection takes place; (2) the quality of interconnection; and (3) the prices charged for interconnection. The necessary conditions for the efficient sharing of data are likely to be at least as complex. Which data would be shared, at what frequency, and at what level of aggregation, as well as the technical standards through which data sharing would take place and the prices, if any, that would be charged by the initial collectors, are among the issues that would have to be addressed in any mandatory data sharing regime.”<sup>78</sup>*

Matters of digital platform interconnection require a specialized expert agency since the platforms are beyond the scope of the FCC and the FTC’s jurisdiction is constrained.

Meaningful interoperability in digital markets often requires access to specific data that enables those who rely upon a platform to reach their customers, place advertisements on specific websites or adjacent to targeted content, or just connect buyers and sellers. As Professor Fiona Scott Morton and David Dinielli point out, dominant display advertising platform assets controlled by Google can be used to deny access to the data necessary for a competitive market to function:

*But without the ability to know who a consumer is and the ability to measure their action that third-party cookies had allowed, advertisers as well as rivals in the ad tech stack will not be able to bid efficiently. Nor will they be able to deliver payment to effective ads (attribution) based on consumer clicks or actions. They will be competing as if they are blind, against a competitor with 20/20 vision.<sup>79</sup>*

Scott Morton and Dinielli discovered a similar problem with how Facebook can control access to data in manners that impede competition:

<sup>78</sup> *Id.*, at 77–78, 79 (citations omitted).

Matters of digital platform interconnection require a specialized expert agency since the platforms are beyond the scope of the FCC and the FTC's jurisdiction is constrained.

*Facebook controls, in addition to its vast stores of user data, all information related to ads placed on its inventory, including click-through rates and the like. Advertisers, despite purchasing ads on Facebook, cannot get Facebook to give them these data, even though Facebook does provide log-level data about ads placed on other properties. This makes it difficult for advertisers to evaluate the actual value of what they are buying. An ad served on a page opened by a bot, for example, does the advertiser no good, nor does an ad at the bottom of a page this is never viewed by the user, or an ad that runs too fast for the human eye to see. But the advertiser does not know how frequently that happens because Facebook refused to share data that permits truly independent third-party audits. This practice is only possible due to Facebook's market power.<sup>80</sup>*

Interoperability requires both cooperation between and among actually or potentially competitive enterprises and informed consumers. Thus, the DPA must use tools known to expand competitive opportunities through standards for data disclosure, transfer, and portability as well as guidance about the distribution of costs among commercial entities that interoperability will invoke. In addition, these standards should enable informed choice and require transparent disclosures of what data are gathered and how they are used. This includes user control over the transfer of personal information and information involving interactions with others, often described as the “social graph.” Transparent disclosures and portability would reduce the cost of switching from platform to platform, reducing impediments to platform competition.

Portability of data also requires technical platform adjustments to ensure that data handoffs work effectively in real-time and with appropriate privacy and security protections. In order to transfer data in a safe and efficient manner, platforms must develop common application programming interfaces (APIs) to manage the process.

The value of data interoperability and portability was demonstrated by one of the most important pro-competitive telecommunications regulations: the FCC's “number portability” rules. Without the ability for consumers to take their phone number to a new carrier if they wanted to switch, telecommunications competition would have been dramatically hampered. The original FCC rule required substantial reengineering of networks and databases to enable a quick handoff between carriers competing to sign up customers. The digital market equivalent would open access to data as well as give consumers the power to port their data from platform to platform could enable innovations that challenge the largest digital market players.

### **Self-Preferencing Practices**

Dominant platforms may condition access to their most essential or critical services through contract or business arrangements. This tends to reinforce the dominant

<sup>79</sup> FIONA SCOTT MORTON & DAVID DINIELLI, ROADMAP FOR A DIGITAL ADVERTISING MONOPOLIZATION CASE AGAINST GOOGLE, Omidyar Network (May 2020), <https://www.omidyar.com/sites/default/files/Roadmap%20for%20a%20Case%20Against%20Google.pdf>.

<sup>80</sup> SCOTT MORTON & DINIELLI, *supra* note 65, at 34.

The value of data interoperability and portability was demonstrated by one of the most important pro-competitive telecommunications regulations: the FCC’s “number portability” rules.

firm’s existing advantages in scale, scope and data dominance over competitors and potential market entrants. The most problematic limitations include exclusive distribution agreements, prohibitions on offering price discounts to competitors, and price or service inducements that favor the dominant platform.

For example, a platform may have used its bottleneck power to negotiate a contract with business customers (app developers on an app store, or retailers on an e-commerce platform) that conditions access to transaction data. The Stigler Report examines how this type of condition could have anticompetitive effects.<sup>81</sup> If the dominant platform also competes against those business customers on its own platform (e.g., selling apps on its own app store, or being a retailer on its own e-commerce marketplace) there’s likely an incentive to use the retailer’s data to benefit the platform’s own plans. “That data advantage over rivals can enable a company to achieve and/or maintain critical economies of scale, better predict consumer behavior, and form a powerful barrier to entry for potential competitors.”<sup>82</sup> The platform could use that data to learn which products are selling well and enter the market niche of the business customer, either through acquisition or new product development. It could use data to learn about the customer’s strategies and how effective they are, either copying them or avoiding them as the data indicates. It could use that data to identify customers and to compete directly, thereby disadvantaging competitors’ ability to target and expand their customer base. The European Union has investigated Amazon for precisely such practices.<sup>83</sup>

A similar effect occurs when a platform company requires installation of a bundle of affiliated products on the platform in order to block the growth of rivals. A platform with its own operating system, for instance, might bundle a set of its own apps because those are the apps which face real or potential competition. When a dominant firm is setting up these bundles, an antitrust case may be ineffective in protecting competition due to the complexity of the problem—e.g., “which apps do consumers really prefer?”—and the slow pace of litigation, as the Microsoft experience evinces. For an existing regulatory agency, the nature of these dangers may not be new, yet the complexity of separating legitimate technical digital business decisions from competitively harmful practices requires the constant focus and vigilance of a specialized agency.

Self-preferencing could have significant impacts throughout the economy in the context of e-commerce or the “Internet of Things.” Consumers must be able to change their defaults, make choices, and connect to unaffiliated products and services in a practical way. Only by weighing the pros and cons of what it takes to synchronize competition, innovation, security and consumer convenience on a day-to-day basis will it be possible to govern digital platforms appropriately.

### **Data Practices**

The commercial advantages and potential abuse of consumer privacy that flow

81 STIGLER ANTITRUST REPORT, *supra* note 12, at 94.

82 *Id.* at 95.

83 Adam Satariano, *Amazon Set to Face Antitrust Charges in European Union*, N.Y. TIMES (Jun. 11, 2020), <https://www.nytimes.com/2020/06/11/technology/amazon-antitrust-european-union.html>.

Only by weighing the pros and cons of what it takes to synchronize competition, innovation, security and consumer convenience on a day-to-day basis will it be possible to govern digital platforms appropriately.

from massive aggregation and control of data by digital platforms of all sizes must be addressed with a cohesive public oversight structure. Consumers today suffer from both a lack of control over how their data are used and an inability to take their data from platform to platform. At one extreme, efforts to protect privacy by simply locking data within the vaults of a dominant platform harm legitimate business opportunities for competitors as well as socially useful research activities. At the other extreme, efforts to allow data to flow openly across markets might compromise data security and privacy. A new agency would be well positioned to balance privacy and competition.

The activities of the DPA should be supportive of whatever Congress decides on privacy policy. Such ongoing legislative activity is focused on establishing the privacy rights of citizens. This paper does not address those issues, but rather the marketplace effects of the use of personal data.

Such marketplace effects include a duty to design digital products in a manner that identifies privacy and security impacts and then mitigates their harms. The Agency must also enable individuals to securely transfer their data from one company to another and delete it from the original company's servers. Companies should also be required to hold an individual's data in trust, instituting protections necessary to assume that the trust is not violated by unauthorized access to the information.