# Aff Wiki Doc

# 1AC

## 1AC – Texas

### 1AC – APIs

#### Advantage one: APIs

#### Dominant digital platforms shut out competition by restricting Application Programming Interfaces (APIs) – mandating interoperability between competing platforms enables market entry.

Sharma ’19 [Chinmayi; JD @ UVA Law; “Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability,” *University of Memphis Law Review*, 50(2), p. 441-508; \*Edited for Gendered Language]

II. APIs and an Interoperable Internet

Understanding how APIs operate can elucidate how they contribute to interoperability and why interoperability is important for a healthy online marketplace. APIs are neither the secret sauce that originally led to an online platform's rise to prominence, nor are APIs the bread and butter that drives a platform's continued success. Rather, they act as gatekeepers to the information bank account fueling all business activity, limiting access through their lock and key design. And as with banks, they allow the owner to benefit from opening access to this stockpile to others who would pay to use it. They represent a two-way dataflow: opening access to third parties to internal data and features, while receiving valuable user information from those third parties about their user activity. Essentially, the code reflects and fosters an organic, symbiotic relationship.

A. What is an API?

Over 1.5 billion websites are registered on the Internet, 32and all of them interact with each other to some degree to provide their unique services. For example, for a single web search, an Internet browser needs to access Bing. Bing then links to the websites in the search results, and these websites often rely on CAPTCHA to verify that the person conducting the search is not a robot. Each task is accomplished by a different entity, but each entity relies on information provided by the others information communicated through APIs. The Internet has been called an information highway, a digital infrastructure, or even a set of pipes. But ultimately, it is nothing more than a series of protocols designed to foster the creation and transfer of information, or data, as described above.

These protocols comprise the fabric of the Internet. They enable programming languages to build applications, enable data transfers necessary to connect with other Internet users, and enable shared access to public or proprietary tools to carve out new digital spaces. 33Previously, these protocols were born of necessity and expanded to achieve [\*451] greater efficiency and innovation among developers collaborating to realize the dream of a powerful open Internet. 34But, as with all good inventions, the Internet was quickly conquered by commercial entities that then used and created new protocols to further their business ends. 35 The collection of these protocols that broker interactions with a particular entity on the Internet are referred to as Application Programming Interfaces (APIs), or libraries of protocol layers. 36

APIs are the connective tissue that allow the various platforms in our digital economy to request and send information to each other. 37 Individuals utilize APIs when using their computers to interact with other computers by sending their information, in the form of an API call, to receive external information. For this to work, networked computers must be ubiquitously accessible and process the individual's request, or API call, in standard protocol to ensure communication. 38 To ensure that their APIs are openly accessible, companies publish documentation outlining how their API is designed, what kind of information third parties can access, the manner in which they have to make the call to receive a reply, and the terms of use for the API. 39

[\*452] In short, standardization feeds interoperability a feature that is not anomalous to the digital sphere. In fact, the vast majority of consumer products are aggregations of disparate patented technologies packaged together. They function because they have been built according to standards formally set by competitors in contracts. 40For example, the manufacture of a single laptop can necessitate adherence to between 250-500 interoperability standards. 41But, while a laptop is a discrete product with finite parties to invite to a standard-setting negotiation, the number of potential parties interacting with any given website can be near infinite. For example, Yelp as a platform needs to interact with Google and Apple Maps to provide directions, OpenTable and Resy to facilitate making a reservation, a phone's GPS to determine proximity, a phone's keyboard to allow users to post reviews, and thousands of advertising providers that pay to post commercials. With the multitude of players involved in any given digital interaction, formal standard-setting procedures common for market players like Dell and Apple are impractical for the digital market. 42Instead, websites like Yelp, Google, Apple, and the other aforementioned entities publish their APIs. 43

[\*453]

B. Interoperability Fosters Competition

The symbiotic relationships fostered by APIs enhances competition in the digital marketplace. Interoperability can have three types of effects on competitive markets:

(1) Direct, in which increased use increases the value of the product itself; (2) indirect, in which increased use leads to development of complementary products, such as applications for a specific platform, which in turn increases the value of the product; and (3) two-sided, in which increased use by one set of users increases the value of a complementary product and vice-versa. 44

Economists widely recognize the formidable hurdle of entering online markets as a feat that "requires either building up strong brand recognition to draw users to an independent site," a resource intensive route, "or using an existing platform," 45 an option made possible by permissive APIs. Innovative products and new startups built off existing platforms use permissive APIs to gain a foothold in a tumultuous market. In turn, the original platforms increase in value and experience an influx of new users. As the saying goes, "rising tides raise all ships."

Interoperability also lowers the barrier of entry to the online marketplace by encouraging the development of complementary platforms. 46At the early stages of the Internet, online platforms were united in their pursuit for active, loyal user bases and collaborated with [\*454] each other to accomplish these goals. 47APIs helped broker these cooperative, pro-competitive strategies. For example, Instagram has witnessed the advent of Instagram celebrities, or individuals who appear to have accumulated overnight fandom teaching people to "be yourself." 48In reality, they are the success stories of third-party apps that allow for planned posts, 49follower analytics, 50and trend-worthy Boomerangs. 51These third-party apps rely on Instagram's API to pull information about users and push information such as curated content. Instagram and these third-party apps mutually benefit from the traffic generated. Security apps have also flourished because platforms like Instagram are reliant on them, 52recognizing platforms sink when users feel unsafe.

The pro-competitive benefits of this "rising tides raise all ships" approach to API design extend beyond encouraging the development of complementary products. Platforms with more universally beneficial services or information can offer access to their APIs for a fee. 53 [\*455] This type of open access to platforms allows for more options to flood the market, theoretically driving out poor quality options that are unable to generate sufficient value to bear the cost of using the API. For example, Google provides its Maps product to developers at a price based on use. 54This allows developers to put Google Maps on their websites and enables users to get directions to a location directly from their app without going to Google. 55The developer pays for this use at a cost proportional to the traffic ~~his or her~~ [their] third-party product generates. 56 This has created an economy of map-based applications that detect potholes, warn of anomalous traffic, and suggest new restaurants, without the new companies having to recreate Google Maps from the ground up. 57

C. Shut Out of the "Walled Gardens"

The concentration of the Internet marketplace in the hands of a few players removes incentives to maintain interoperability, making the issue unlikely to self-correct. As online companies mature, the marginal utility of additional exposure via third-party applications becomes outweighed by the potential benefits of restricting open access to proprietary information to stifle future competition. 58Thus, dominant [\*456] players are shifting to "walled garden" models, restricting API access and diminishing Internet interoperability. 59"Walled gardens" refer to platforms that, previously open, now substantially limit third-party access to their information and services with code-and contract-based barriers. 60Some deride this shift to "walled gardens" as the dystopian antithesis of open Internet goals, 61while others see "walled gardens" as the natural end point of company maturation and the development of a sustainable revenue model. 62Ideology aside, "walled garden" APIs definitively reduce interoperability by setting up formidable barriers to third-party access of platform data, reducing innovation of platform-dependent apps and equipping these dominant players with the ability to unilaterally alter API conditions. 63

An already concentrated online market engenders further concentration. For one, venture capitalists ("VCs") have driven market concentration. The tech sector contains many startups not projected to [\*457] turn a profit for years, entirely reliant on external investments. 64At first, VCs took gambles on nascent companies with potential, focusing on their "exit" potential (or acquisition by a dominant player). 65 Later on, VCs began concentrating their funding on a smaller number of more mature tech companies rather than spurring innovation by funding embryonic startups. 66And now, well-funded market players, either through VCs or through initial public offerings ("IPOs"), have the ability to buy out future competitors and acquire complementary products to internalize their features. 67After a major merger or acquisition, tech companies undergo massive reorganizations to accommodate the new company, including a transformation of APIs to begin the process of integrating the new addition's technology into a legacy system. 68 APIs [\*458] were designed to facilitate mutually beneficial information transactions between competitors, but when one company buys up Park Place and Boardwalk in Monopoly, they no longer have an incentive to cooperate with others.

Companies can reduce interoperability by restricting API access after an acquisition. For example, after Facebook acquired Instagram in 2012 for $ 1 billion, it immediately began integrating the platform into traditional Facebook features. 69Notably, it altered Instagram's API within months of the purchase to prevent users from cross-posting photos generated for Instagram onto Twitter, thereby preventing Twitter users from accessing Instagram content directly. 70Facebook's goal was to drive activity to Instagram's native platform directly rather than have users interact with Instagram content through other, and at the time more dominant, social media avenues. 71But in doing so, Facebook hurt Twitter's dynamism as a platform by reducing Twitter's access to high-quality, third-party content. 72In response, Twitter deleted its app from the Facebook ecosystem. 73 Instagram's newly restrictive API halted the trend of building one-off, third-party projects, such as hashtag driven campaigns or event promotion. 74

[\*459] In a concentrated market with a dearth of options, dominant players can further reduce interoperability by making the conditions of API access prohibitive. Although tech companies are notorious for evading profitability for unfathomably long periods of time, all companies ultimately seek revenue. Google Maps's API, one of the most dominant geolocation services available, has recently capitalized on the market's reliance on its services to increase the price associated with making API "calls" or discrete requests for information. 75When controlling for quantity and cadence of API calls, developers reported an over 1,400% increase in the costs for using the Maps platform. 76In addition to these increased costs, Google has required API users to hand over billing information regardless of whether or not they incur any costs. 77Most significantly, native Android app developers are protected from these changes because Google will not be implementing these new cost structures in its Mobile Native Static and Dynamic Maps APIs the unique APIs built for use by Android developers. 78Ergo, Google, through its APIs, demonstrates favoritism or exceptionalism for the mobile operating system it owns.

Restrictive APIs are by no means per se unreasonable or anticompetitive. Most online platforms generate revenue through advertising, and the "walled garden" model helps platforms curate more personalized, effective advertising schemes. 79Additionally, restricting [\*460] access to APIs limits the ability for low-quality third-party applications to dilute the company's brand by association. 80Finally, data security concerns have also driven decisions to fortify "walled gardens." 81Facebook and Facebook-owned Instagram responded to the Cambridge Analytica data leak and API-enabled data breach by severely curtailing third-party access to user information by putting restrictive conditions on their APIs. 82This move gave Facebook more control over who is accessing information, how much information they are accessing, what they plan to use it for, and whether they are complying with API use conditions. 83Users were duly indignant at the open and unmonitored nature of APIs, but the appropriately placed frustration has since evolved into the belief that there is an unavoidable zero-sum game between interoperability and information security. 84

Just as all monopolies are not per se injurious to competition or the public, 85not all API-restricted walled gardens are problematic. But, [\*461] as with monopolies, we rely on competition law to redress impermissible business practices. The question remains: can it?

#### Interoperability creates platform competition by reducing network effects and switching costs – it allows users to leave platforms without losing ability to interact with them.

Chao ’20 [Becky; 5/13/20; Fellow in Open Technology Institute @ New America; Former Millennial Public Policy Fellow @ OTI, Former Honors Paralegal in Bureau of Competition @ Federal Trade Commission, BA in Public Policy @ Duke; and Ross Schulman; Senior Counsel and Senior Policy Technologist in Open Technology Institute @ New America, JD @ American University, BS in Computer Science @ Brandeis University; “Promoting Platform Interoperability”; https://www.newamerica.org/oti/reports/promoting-platform-interoperability/]

Online Platform Competition Is Hard to Address

Online platforms possess unique gatekeeping power. By setting API design and policy, they have the ability to control who has access to critical aspects of the vast datasets and user bases they’ve built—things like a user’s social graph that enables a hopeful competitor to grow its own user base and establish itself. Once a platform is sufficiently scaled, and especially if it is dominant, it no longer has the incentives to grant access to its APIs to facilitate a healthy downstream ecosystem. The more vertically integrated a platform is, too, the higher the risk that it may not offer APIs with sufficient data and functionality for other companies.20 Whereas our current antitrust framework may not sufficiently ensure platform competition, platform interoperability offers a solution to promote a more competitive ecosystem.

Platforms Operate in Multi-sided Markets and Benefit from Network Effects

Online platforms do not always offer a single product or service, but often build complex businesses across a wide range of commercial offerings. This business model includes many business lines that are vertically integrated on top of one another—meaning that a single company controls more than one stage of the supply chain. Google’s advertising intermediation business, for instance, is largely vertically integrated in that it operates: (1) as a publisher ad-server (offering advertisers the opportunity to run ads on Google’s digital properties—anywhere from alongside certain Google search results to on Google’s websites, such as Gmail, Blogger, and Youtube)21; (2) as a supply-side platform selling inventory on behalf of publishers (optimizing inventory usage through Google’s Ad Manager to maximize ad views); and (3) as a demand-side platform buying inventory on behalf of advertisers (offering advertisers access to display, video, and mobile inventory in real-time through Display & Video 360, formerly DoubleClick Bid Manager).22

Online platforms are complex, but they share several characteristics that distinguish them from traditional brick-and-mortar businesses. Public Knowledge Vice President Harold Feld defines a digital platform as a product that meets the following criteria: “(1) a service accessed via the internet; (2) the service is two-sided or multi-sided, with at least one side open to the public that allows the public to play multiple roles (e.g., content creator as well as content consumer); and (3) which therefore enjoys particular types of powerful network effects.”23 Because these platforms deliver services over the internet, they are able to take advantage of economies of scale. Their costs of scaling the network are dramatically reduced compared to brick-and-mortar businesses that have to build out a physical network to reach customers.24 In addition, operating in a two-sided or multi-sided market reduces a firm’s costs for inventory and market research.25

Online platforms also enjoy network effects, which further entrench their market dominance. A network effect means that the value of the network increases with each additional participant. Through the internet, platforms benefit from being able to reach greater numbers of other users and businesses. When platforms operate with closed systems, such network effects can also affect competition. For instance, Facebook’s network effects from the 2 billion plus users on its network means that users may be reluctant to leave it for a competitor, especially if it means that the user has to expend substantial switching costs by rebuilding their personal networks, posting content, and more from scratch.26 Switching costs and network effects can therefore lock in a user by making them dependent on a particular firm’s good or service.

Given these dynamics, the dominance of a few online platforms reflects an unsurprising trend toward greater concentration. The rise of these platforms, in fact, can be attributed to hundreds of mergers consummated in rapid succession.27 Platforms are keen to capitalize on economies of scale and tap into network effects, especially through vertical integration and data consolidation.28

#### Dominant platforms will control smart cities – that ensures project failure since the public won’t buy in.

Scammell ’21 [Robert; May 2021; Deputy Editor @ Verdict; “Big Tech’s smart city power grab”; https://magazine.verdict.co.uk/verdict\_magazine\_may21/big\_tech\_smart\_cities]

Cities need to become smarter if they are to support soaring populations. The UN predicts that 68% of the world’s people will live in urban areas by 2050, up from 55% today. And with the human population expected to near 10 billion by 2050, making efficient use of every inch of city space is high on the agenda of local governments.

All this makes for a market with lucrative potential for the companies providing the technology solutions powering the cities of the future, from smart waste management to autonomous delivery robots. According to GlobalData estimates, the smart city market will be worth $833bn by 2030, up from $441bn in 2018.

More specialised industrial companies such as Siemens, Hitachi and General Electric have traditionally ruled this sector. However, powerful tech companies from conventionally consumer markets are increasingly expanding onto industrial firms’ turf in pursuit of new revenue streams.

“Big Tech wouldn’t be in smart cities if it didn’t see it as a money-making opportunity,” says David Bicknell, principal analyst at GlobalData’s thematic research team and smart city expert.

But what tech companies see as diversification, critics perceive as a power grab in nascent markets from companies already accused of throttling competition in their own sectors.

“There are already fears that companies that gain an early foothold in smart cities will come to dominate so-called urban technology, just as the early days of the internet were dominated by proprietary solutions before a more open approach took over,” noted GlobalData thematic researchers in a 2019 report on smart cities.

Google-owner Alphabet and Amazon are, for instance, making moves into smart cities while simultaneously already battling multiple antitrust probes on both sides of the Atlantic. Their detractors fear that their financial muscle and deep data resources could empower them to control the growing industry.

Google has captured 90% of the search engine market, which in turn allows it to form one half of the Facebook-Google digital advertising duopoly. Now, Alphabet is trying to do the same in smart cities.

Among the tech giant’s many projects is Sidewalk Labs, an urban planning and infrastructure subsidiary. Its mission is to “make cities more sustainable and affordable for all” by creating products, investing in new companies and taking an active role in designing city spaces.

Ecommerce giant Amazon has a smart cities project in the works, also called Sidewalks. It uses select Amazon home devices to create a “neighbourhood network” running on Bluetooth Low Energy and other frequencies to extend internet connection beyond the home.

AWS, the online retailer’s cloud computing powerhouse, is also working with the City of Chicago on OpenGrid, a real-time, open-source situational awareness program intended to improve the efficiency of city operations.

It is often said that data is the new oil. Less often, it is pointed out that data, unlike oil, has a potentially infinite supply. As more and more sensors are added into city spaces the vendors controlling that data pool could, in theory, use it to gain a competitive advantage in other areas. Amazon has form in this area; one of its antitrust charges accuses it of benefiting from its dual role as platform for other sellers and a retailer of its own goods, using third-party data to inform its own retail decisions.

Even with anonymised datasets, a tech company could glean aggregated insights that boost its business interests elsewhere – and make it harder for smaller startups to break into the smart city space. This also presents concerns about how the technology could be used by authoritarian regimes to control their citizens.

Surveillance state of mind

Beyond the business ramifications, privacy campaigners have been ringing the alarm bell over Big Tech’s growing role in urban spaces.

“We have observed the emergence of a narrative that says systematic data generation, collection and centralisation are the answers to all problems,” says Eva Blum-Dumontent, senior research officer at Privacy International. “This narrative – promoted by companies that sell data processing and AI to local governments – has led to the very real and concrete transformation of our cities into increasingly surveilled public spaces, as well as places of exclusion and discrimination.”

Surveillance facilitated by Big Tech is most prominent in China, where computer vision, facial recognition and AI track the movements of citizens and feed them into the Skynet mass-surveillance network. This, in turn, is closely linked to China’s Social Credit System, a government database that scores citizens on their trustworthiness by following their every move and interaction across the city.

These privacy concerns are intimately linked to the involvement of China’s homegrown tech giants in urban spaces. In 2018 four Chinese tech giants – Ping An, Alibaba, Tencent, and Huawei – launched PATH, an initiative to help 500 Chinese cities become smart cities.

In Hangzhou, ecommerce behemoth Alibaba operates its City Brain system, which uses AI to manage transportation networks. It was given control of 104 traffic light junctions in the city’s Xiashoshan district and its algorithms were able to increase traffic efficiency by 15% in its first year.

While Alibaba Cloud provides the software, the city owns the data. But when the state is authoritarian, it raises further questions about the relationship between Big Tech and big government.

This murky relationship moved to centre stage for Chinese telecommunications giant Huawei. One of China’s biggest tech players, it is one of the leading providers of 4G and 5G equipment. Until a couple of years ago its spread across the globe seemed unstoppable. That growth began to unravel in 2019 after the questioning about Huawei’s ties to the Chinese state reached a boiling point.

Critics pointed to its founder’s past in the Chinese military, the state subsidies it had received and Chinese national security law that could, in theory, compel the company to give government access to communications on its network. Huawei has consistently denied accusations that it poses a national security threat. The absence of a smoking gun did not stop the company from being ostracised across the West. Above all, the saga underscored an admission from Western governments of the critical role that tech companies play in city infrastructure – and the risks they could pose, real or hypothetical.

Privacy on the ropes

Smart city surveillance is not limited to China. In 2019, developers at King’s Cross, London, sparked outrage after it emerged passersby were being monitored by live facial recognition installed in CCTV cameras. The system had been installed in secret and without any oversight from the police, prompting an investigation by the UK’s data regulator.

While the live facial recognition software was not provided by Big Tech, such companies are providing surveillance systems elsewhere. More than 2,000 police and fire departments in the US have partnered with Amazon’s Ring camera system, which effectively turns a consumer camera into an extension of a state surveillance network – all facilitated by Big Tech. Amazon has given out thousands of free Ring devices as part of an initiative with UK police.

Amazon’s relationship with law enforcement doesn’t stop at hardware. Its facial recognition software, Rekognition, is based on AWS technology and had been sold to law enforcement across the US. In June 2020 it put a one-year moratorium on selling Rekognition to police after civil liberty groups raised concerns about the tech’s potential racial bias. IBM, facing similar pressures, also paused the sale of its own facial recognition software to police.

These reactions, along with protestors in Hong Kong tearing down smart streetlights, demonstrate a fierce backlash to smart city technology when citizens believe the technology poses more risks than benefits. But there is one episode that has become a case study for backlash against Big Tech in smart cities.

The Sidewalk saga

Google Sidewalk Lab’s Quayside project in Toronto was championed by Canadian Prime Minister Justin Trudeau and Google co-founder Eric Schmidt as a community built “from the internet up”.

First proposed in October 2017 as a 12-acre neighbourhood, it aimed to become a truly smart city with features such as “snow-melting roadways”, an “underground delivery system” and homes that used cutting-edge wood-frame towers to make housing more affordable

But over the next two years the project unravelled. First, tensions mounted when Sidewalk Labs increased the size of the neighbourhood to 190 acres. There were also disagreements in vision between the Google company and Waterfront Toronto, the organisation managing the renovation. But the biggest backlash came from residents, who feared their data would be collected and stored by the tech goliath.

“No matter what Google is offering, the value to Toronto cannot possibly approach the value your city is giving up,” wrote venture capitalist Roger McNamee in a letter to the Toronto city council at the time. “It is a dystopian vision that has no place in a democratic society.”

Despite promises by Google that citizen data wouldn’t be shared with third parties, the backlash continued.

The project closed in May 2020, with the uncertainty of the Covid-19 pandemic given as a reason. But GlobalData’s Bicknell says the biggest factor in its demise was “data privacy”. And the episode could have wider implications for smart city projects, he says.

“The failure of that project overshadows other good smart cities engagements,” he explains. “It was a high-profile project and the data privacy concerns will chime with other cities and citizens.

Smart cities working for everyone

Big Tech’s role in smart cities seems unlikely to go away. So how can it be ensured that it works for citizens and not for Big Tech’s balance sheet?

First, it is worth highlighting that not all smart city projects pose immediate risks, whether it’s data privacy or market dominance. For example, last year Vodafone partnered with SES Water to fit water pipes with narrowband IoT sensors that monitor pressure, flow, temperature and acoustic signals to detect leaks. The project aims to reduce water leakage by 15% in five years, which could save billions of litres of water per day – something residents are unlikely to take issue with.

As countries look to reopen from the pandemic, the management of city spaces will be key to ensuring a balance between safety and a return to normality. Smart city tech could be part of that solution, but according to GlobalData’s Bicknell it would be wise for Big Tech to be cautious in their involvement.

“Maybe cities, for now, just need to be resilient rather than smart” he explains. “Big Tech can help. It can bring new thinking, scale and ideas, for good. What it can’t do is be seen to be a behemoth overshadowing projects, which is arguably what happened in Toronto. Big Tech wasn’t the solution. It was the problem.”

Justin Bean, global director of smart cities and smart spaces at Hitachi Vantara, tells Verdict that there’s clearly a “gap in trust between citizens, business and government”.

#### Interoperability ensures open access to data between competitors in smart cities – that enables innovation that makes urbanization sustainable.

Ahlgren ’16 [Bengt et al; Senior Researcher in the Decisions, Networking, and Analytics Lab @ SICS Swedish ICT, PhD in Computer Systems @ Uppsala; Markus Hidell, Associate Professor in Communication Systems in Network Systems Laboratory @ KTH Royal Institute of Technology, PhD in Telecommunication @ KTH Royal Institute of Technology; Edith C.-H. Ngai, Associate Professor in the Department of Information Technology @ Uppsala University, PhD in Computer Science and Engineering @ Chinese University of Hong Kong; “Internet of Things for Smart Cities: Interoperability and Open Data,” *IEEE Internet Computing*, 20(6), p. 52-56]

Today’s cities face a variety of challenges, including job creation, economic growth, environmental sustainability, and social resilience. Emissions from motor vehicles have become a major source of air pollution in the world’s large and medium-sized cities. Many large cities experience serious air pollution and greenhouse gas emission (GHG), which is made worse by increasing traffic congestion. With these challenges in mind, the European Union and many other countries are investing in information and communication technology (ICT) research and innovation, and developing policies to improve the quality of life of citizens and sustainability of cities. Given the trend of ICT for smart sustainable cities, understanding where we are in the evolution of the Internet is critical to future city-planning processes.

The Internet of Things (IoT) has been viewed as a promising technology with great potential for addressing many societal challenges. Cisco believes that many organizations are currently experiencing the IoT, the networked connection of physical objects and the cyberspace.1 According to the International Data Corporation (IDC)’s Worldwide Internet of Things Forecast, 2015–2020, 30 billion connected (autonomous) things are predicted to be part of the IoT by 2020 (see www.idc.com/infographics/IoT). The IoT market size is forecast to grow from US$157 billion in 2016 to $661 billion2 by 2021. The adoption of cloud platforms, development of cheaper and smarter sensors, and evolution of high-speed networks are expected to drive the growth of the IoT market.

Many cities, such as London and New York, see the increasing need and interest of the public sectors to explore IoT technologies to improve traffic flow, reduce pollution and energy consumption, and collect data for policing. Smart cities are an urban development vision to integrate multiple ICT solutions to manage a city’s assets to create a sustainable environment, improve the quality of life, and enhance efficiency and economical value. The number of new IoT products and applications has grown exponentially in recent years. Various communication standards and protocols have been suggested in the community, and some have been adopted in different IoT devices. However, there are also quite a few proprietary protocols and cloud services in the IoT, which make the interoperability and sharing of data across different devices and platforms quite challenging. Open data in smart cities means not only global data collected and opened by the government, but also includes the sharing of data among individual citizens and industries with the government and general public. In this article, we’ll discuss the advantages of open data and standards within the IoT, current limitations, and future trends.

IoT for Smart Cities

The IoT provides individuals, society, and the business world new opportunities to access volumes of data and to develop new applications and services for creating a cleaner environment and more intelligent society.3 The information society is rapidly becoming a central pillar for urban planners, architects, developers, and transportation providers, as well as in public service provision. One good example is using smartphones and smart meters to regulate energy consumption in the Hyllie smart networks of Malmö, Sweden.4 The system enables people to measure, monitor, control, and influence their own energy consumption, and be able to independently produce renewable energy (for example, by using solar panels). One way to optimize the use of renewable energy and reduce costs is to decide how and when you want to charge your electric car. Consumers are informed of the supply of renewable energy in the system and how much electricity costs via smartphones or tablets.

From a public sector leadership perspective, cities can be viewed as microcosms of the interconnected networks for building a clean, energy-efficient, and sustainable society. In Amsterdam, a network-enabled LED streetlighting system has been developed to reduce the city’s energy consumption and costs.5 Similarly, in the US, Cisco and a wide range of public and private stakeholders in Chicago have been driving smart community initiatives to improve neighboring services and the quality of life.6 IoT solutions are more effective when they facilitate open data and encourage public engagement, to achieve the goals of increasing productivity, decreasing costs, and improving citizens’ quality of life.

Interoperability and Open Standard Development

With the popularity of IoT devices, many IoT protocols and standards have been developed. In contrast to ordinary computers, IoT devices are normally constrained when it comes to memory space and processing capacity. In addition, IoT devices might be deployed where there’s limited or no access to continuous power supply, which means that they need to operate under power supplied from batteries or small solar panels. As a consequence, power-efficient communication protocols with small memory footprints and limited demands on processing have been developed to support IoT devices. Traditional TCP/IP protocols haven’t been designed with these requirements in mind. Over the past years, however, IoT protocols have been standardized on virtually all layers of the protocol stack. These protocols typically have low complexity as an important design goal and are optimized for constrained environments.

Table 1 shows a few examples of IP-based open protocol standards commonly used for IoT communication. For instance, IEEE 802.15.4 has been widely adopted in many smart devices as the MAC and Physical layer protocol. Several network layer and application layer protocols have also been proposed for constrained devices. Standard protocols are important to guarantee interoperability of different IoT devices.

However, using open standards doesn’t automatically result in open systems. In our context, an open system means an integrated open IoT infrastructure solution for smart cities, providing access to open data and APIs for cloud services. In many cities, that infrastructure will be paid for, at least in part, by the city authorities using public funding. To motivate this investment, and get the most benefit for society, we argue that any smart city IoT infrastructure needs to be a truly open system, where equipment from many vendors can be used, and where the generated data can be more or less freely used by anyone to develop new services, based on low-level as well as processed sensor and IoT data. This kind of system will maximize innovation in the IoT domain, much as the Internet has done for information and communication services.

Many current IoT systems — for example, for air quality monitoring or the smart home — are either incomplete systems with limited functionalities (that is, in terms of sensing, storage, and analytics), or are closed, proprietary systems dedicated for a particular task. The latter are vertically integrated systems, sometimes called stove pipes or vertical silos, which can’t be combined or extended easily with third-party components or services. The result is that once invested in a particular system, you’re locked into that vendor’s system. Vertically integrated systems are particularly problematic for the public sector, because this prevents fair competition in public procurement and is less suitable for large-scale data sharing.

Patrik Fältström7 argues similarly that market forces work against open interoperability, especially in the IoT domain where, for example, a smart lighting system from one vendor only works with light bulbs from the same vendor. Systems are designed as end-to-cloud-to-end, where the cloud part is vendor-controlled with limited possibilities for third parties, and where the IoT devices often speak proprietary protocols to the cloud. Fältström argues that this lack of interoperability severely limits the market growth (for example, with smart light bulbs). Also, the dependence on a cloud service might render the device nonfunctional, should that cloud service for any reason, temporarily or permanently, disappear.

Instead of these stove pipes, we need horizontally designed systems with well-defined interfaces and data formats that can unleash the potential of open data, and that enable third parties to independently develop new applications and services, possibly combining several data sources. Providing open data has huge potential for innovation in digital applications and services, resulting in very large economic values. These interfaces (APIs) through which the IoT data can be accessed at multiple levels of refinement — from raw data directly from sensors, to highly processed data — also need standardization. The challenge is to provide an open system that lets users access the open data and cloud services without being locked by a particular platform. The open system should also allow third-parties to innovate based on the open data and open APIs.

Case Study: GreenIoT Project in Sweden

We developed a GreenIoT solution that incorporates smart sensing and cloud computing technologies to encompass a more interactive and responsive city administration with private and public parties. The proposed open GreenIoT platform supports a wide range of applications, such as environmental monitoring, transportation, factory process optimization, and home security, and enables third-party innovation in new IoT-based services. Driven by Uppsala Municipality, we implement and demonstrate GreenIoT as a testbed in the city of Uppsala (the fourth largest city in Sweden) to support air pollution monitoring and traffic planning. Because the particulate level of Uppsala occasionally exceeds the EU standard, in particular during the winter and early spring, one objective is to reduce air pollution through active monitoring, traffic management, and better city planning.

Existing IoT technologies have largely contributed to hardware, software and protocol design. However, a major challenge of the IoT lies in how to extract valuable information from vast volumes of data generated from the smart devices (also known as the “Big Data” problem). Our GreenIoT solution leverages cloud computing to support intelligent data management, and integrate with green networking and sensing techniques to support energy-efficient and sustainable operations. The GreenIoT platform in Uppsala will be based on open standards, open to the public and supporting industries to test their new sensing products. It provides open data and open APIs for third parties to access the sensor data and make use of the cloud services. The open data generated by the smart devices and platform will drive the development of innovative applications and services.

One major goal of the project is an integrated solution for an environmental sensing system, which enables experimentation with applications and services using open environmental data, particularly for sustainable urban and transportation planning (see Figure 1). The GreenIoT architecture is manifested in terms of a testbed in Uppsala. The sensing system and application platform are built from unique technology that provides open interfaces at several levels, energy and resource efficiency, and application independence. We use a unique tool for visualization in four dimensions, which supports smart city simulations and is fully integrated with the sensor data for real-time feedback. The testbed, including the open data and open APIs, allow third parties to develop and experiment new sensing products and services that could be exported to international markets.

To fulfill user requirements — from advanced tools for city planning as well as from novel applications making sensor data useful to citizens — we devised the GreenIoT architecture (see Figure 2).

Data produced by sensor networks are delivered through sensor gateways for storage and processing managed by cloud services for sensor data. The sensors use a publish/ subscribe protocol, Message Queuing Telemetry Transport (MQTT), to communicate data in an open format through a broker for further storage and processing in the cloud, or for direct use by applications and services. We’re also experimenting with information-centric networking8 for direct access to sensor data.

Sensor data can be retrieved by tools and applications through welldefined APIs. The sensor data cloud services support both requests for raw sensor data and for pre-processed sensor data. Pre-processed data can be described as a grid of estimated values for a geographical region, where the values are calculated from the actual data produced by sensors in that region. A set of pre-processing types has been defined, such as interpolated data, hourly average, daily average, and weekly average. These types should be seen as a starting point, and more types are likely to be defined in the future. In the long run, it even should be possible for tools and applications to define processing that can be executed by the sensor data cloud services and then retrieve refined data according to their demands. The open APIs and open data format will facilitate the sharing of open data and guarantee the accessibility of cloud services without relying on a single device manufacturer or service provider.

The vision of the “smart city,” making use of the IoT to provide services for the good of citizens and public authorities, promises solutions to some of today’s societal challenges such as air quality, transportation, and energy efficiency. These IoT systems must be based on open data and open standards, including protocols and interfaces, so that the systems enable third-party innovation in new services, and to avoid vendor lock-in. Standardized protocols might not be enough to achieve these goals — systems must be designed with openness in mind at all levels. Based on this concept, we designed and developed a GreenIoT platform in Sweden to demonstrate the benefits of open data and open platforms for smart city development. Over the next year, we will develop applications and carry out experiments using the Uppsala City IoT testbed, and formulate guidelines for public bodies for the procurement of open IoT infrastructure – including open APIs, common data formats, and how to avoid vendor lock-in. Open systems enabling innovation in new services are particularly important for publicly funded IoT infrastructures, to maximize the benefits for society.

#### Otherwise, extinction.

Cribb ’16 [Julian; Senior Visiting Fellow @ FutureDirections, Former Scientific Editor @ The Australian, Author of *The Coming Famine* and *Poisoned Planet*, Former Foundation President @ Australian Science Communicators Association; “The Urbanite (Homo urbanus)” in *Surviving the 21st Century*, p. 147-169]

A Hand-Made World

By the mid-twenty-first century the world’s cities will be home to approaching eight billion inhabitants and will carpet an area of the planet’s surface the size of China. Several megacities will have 20, 30, and even 40 million people. The largest city on Earth will be Guangzhou-Shenzen, which already has an estimated 120 million citizens crowded into in its greater metropolitan area (Vidal 2010).

By the 2050s these colossal conurbations will absorb 4.5 trillion tonnes of fresh water for domestic, urban and industrial purposes, and consume around 75 billion tonnes of metals, materials and resources every year. Their very existence will depend on the preservation of a precarious balance between the essential resources they need for survival and growth—and the capacity of the Earth to supply them. Furthermore, they will generate equally phenomenal volumes of waste, reaching an alpine 2.2 billion tonnes by 2025 (World Bank)—an average of six million tonnes a day—and probably doubling again by the 2050s, in line with economic demand for material goods and food. In the words of the Global Footprint Network “The global effort for sustainability will be won, or lost, in the world’s cities” (Global Footprint Network 2015).

As we have seen in the case of food (Chap. 7), these giant cities exist on a razor’s edge, at risk of resource crises for which none of them are fully-prepared. They are potential targets for weapons of mass destruction (Chap. 4). They are humicribs for emerging pandemic diseases, breeding grounds for crime and hatcheries for unregulated advances in biotechnology, nanoscience, chemistry and artificial intelligence.

Beyond all this, however, they are also the places where human minds are joining at lightspeed to share knowledge, wisdom and craft solutions to the multiple challenges we face.

For good or ill, in cities is the future of civilisation written. They cradle both our hopes and fears.

Urban Perils

The Brazilian metropolis of Sao Paulo is a harbinger of the challenges which lie ahead for Homo urbanus, Urban Human. In a land which the New York Times once dubbed “the Saudi Arabia of water” because its rivers and lakes held an eighth of all the fresh water on the planet, Brazil’s largest and wealthiest city and its 20 million inhabitants were almost brought to their knees by a one-in-a-hundred-year drought (Romero 2015). It wasn’t simply a drought, however, but rather a complex interplay of factors driven by human overexploitation of the surrounding landscape, pollution of the planetary atmosphere and biosphere, corruption of officialdom, mismanagement and governance failure. In other words, the sort of mess that potentially confronts most of the world’s megacities.

In the case of Sao Paulo, climate change was implicated by scientists in making a bad drought worse. This was compounded by overclearing in the Amazon basin, which is thought to have reduced local hydrological cycling so that less water was respired by forests and less rain then fell locally. This reduced infiltration into the landscape and inflow to river systems which land-clearing had engorged with sediment and nutrients. Rivers running through the city were rendered undrinkable from the industrial pollutants and waste dumped in them. The Sao Paulo water network leaked badly, was subject to corruption, mismanagement and pilfering bordering on pillage. Government plans to build more dams arrived 20 years too late. “Only a deluge can save São Paulo,” Vicente Andreu, the chief of Brazil’s National Water Agency (ANA) told The Economist magazine (The Economist 2014). Depopulation, voluntary or forced, loomed as a stark option, officials admitted. Although the drought eased in 2016, water scarcity remained a shadow over the region’s future.

Sao Paulo is far from alone: many of the world’s great cities face the spectre of thirst. The same El Nino event also struck the great cities of California, leading urban planners—like others all over the world—to turn to desalination of seawater, using electricity and reverse osmosis filtration (Talbot 2014). This kneejerk response to unanticipated water scarcity echoed the Australian experience where, following the ‘Millennium Drought’ desalination plants were producing 460 gigalitres of water a year in four major cities (National Water Commission 2008)—only to be mothballed a few years later when the dry eased. By the early 2010s there were more than 17,000 desalination plants in 150 countries worldwide, churning out more than 80 gigalitres (21 billion US gallons) of water per day, according to the International Desalination Association (Brown 2015). Most of these plants were powered by fossil fuels which supply the immense amount of energy needed to push saline water through a membrane filter and remove the salt. Ironically, by releasing more carbon into the atmosphere, desalination exacerbates global warming and so helps to increase the probability of fiercer and more frequent droughts. It thus defeats its own purpose by reducing natural water supplies. A similar irony applies to the city of Los Angeles which attempted to protect its dwindling water storages from evaporation by covering them with millions of plastic balls (Howard 2015)—thus using petrochemicals in an attempt to solve a problem originally caused by … petrochemicals.

These examples illustrate the ‘wicked’ character of the complex challenges now facing the world’s cities—where poorly-conceived ‘solutions’ may only land the metropolis, and the planet, in deeper trouble that it was before. This is a direct consequence of the pressure of demands from our swollen population outrunning the natural capacity of the Earth to supply them, and short-sighted or corrupt local politics leading to ‘bandaid’ solutions that don’t work or cause more trouble in the long run.

Other forms of increasing urban vulnerability include: storm damage, sea level rise, flooding and fire resulting from climate change or geotectonic forces; governance failure, civic unrest and civil war exemplified in Lebanon, Iraq and Syria over the 2010s; disruption of oil supplies and consequent failure of food supplies; worsening urban health problems due to the rapid spread of pandemic diseases and industrial pollution and still ill-defined but real threats posed by the rise of machine intelligence and nanoscience (Gencer 2013). The issue was highlighted early in the present millennium by UN Secretary General Kofi Annan, who wrote:

Communities will always face natural hazards, but today’s disasters are often generated by, or at least exacerbated by, human activities… At no time in human history have so many people lived in cities clustered around seismically active areas. Destitution and demographic pressure have led more people than ever before to live in flood plains or in areas prone to landslides. Poor land-use planning; environmental management; and a lack of regulatory mechanisms both increase the risk and exacerbate the effects of disasters (Annan 2003).

These factors are a warning sign for the real possibility of megacity collapses within coming decades. With the universal spread of smart phones, the consequences will be vividly displayed in real time on news bulletins and social media. Unlike historic calamities, the whole world will have a virtual ringside seat as future urban nightmares unfold.

#### API interoperability under the antitrust frame key to regulated quantum technology.

Kop ’20 [Mauritz; Stanford Law School TTLF Fellow @ Stanford University, Managing Partner @ AIRecht, Amsterdam, The Netherlands, “Regulating Transformative Technology in The Quantum Age: Intellectual Property, Standardization & Sustainable Innovation” https://law.stanford.edu/wp-content/uploads/2020/11/Mauritz-Kop\_Regulating-Transformative-Technology-in-The-Quantum-Age\_Intellectual-Property-Standardization-Sustainable-Innovation\_Stanford.pdf]

Regulating technology is a continuous effort. It is a dynamic, ongoing process that follows the lifecycle of the technology and the application. The article argues that the pervasiveness of quantum technology asks for a holistic view on a regulatory framework, that balances the interests of stakeholders and that of society at large. It demands for an agile legislative system that can adapt quickly to changing circumstances and societal needs. How can policy makers realize these objectives and regulate quantum computing, quantum sensing and the quantum internet in a socially responsible manner? Regulation that addresses risks in a proportional manner, whilst optimizing the benefits of this cutting edge technology? Without hindering sustainable innovation, including the apportionment of rights, responsibilities and duties of care? What are the effects of standardization and certification on innovation, intellectual property, competition and market-entrance of quantum-startups?

Moreover, which culturally sensitive ethical issues play a role in these regulations? Would it be a good first step to link the governance of quantum & AI hybrids to the Trustworthy AI principles? Do quantum’s different physical properties call for additional core rules? Is it wise to embed our democratic values into the architecture of quantum systems, by way of Trustworthy Quantum Technology by Design? The article explores possible answers to these tantalizing questions. Particles and energy at the subatomic level do not follow the same rules as the objects we can detect around us in our everyday lives. In addition to universal, overarching guiding principles of Trustworthy & Responsible Quantum Technology that are in line with the unique physical characteristics of quantum mechanics, the article advocates a vertical, differentiated industry-specific legislative approach regarding innovation incentives (based on the innovation policy pluralism toolkit), externalities and risks (based on the pyramid of criticality, which should include a definition of highrisk quantum technology applications).

The article demonstrates that strategically using a mixture of IP rights to maximize the value of the IP portfolio of the quantum computer’s owner, potentially leads to IP protection in perpetuity. Overlapping IP protection regimes can result in unlimited duration of global exclusive exploitation rights for first movers, being a handful of universities and large corporations. The ensuing IP overprotection in the field of quantum computing leads to an unwanted concentration of market power. Overprotection of information causes market barriers and hinders both healthy competition and industry-specific innovation. In this particular case it slows down progress in an important application area of quantum technology, namely quantum computing.

In general, our current intellectual property framework is not written with quantum technology in mind. Intellectual property should be an exception -limited in time and scope- to the rule that information goods can be used for the common good without restraint. Intellectual property cannot incentivize creation, prevent market failure, fix winner-takes-all effects, eliminate free riding and prohibit predatory market behavior at the same time. To encourage fair competition and correct market skewness, antitrust law is the instrument of choice.

#### Unregulated quantum tech infinitely multiplies US-Russia-China security dilemma – nuclear war.

Allison ’19 [Kevin; Senior Editor @ Signal; “Why quantum computing could be a geopolitical time bomb,” GZERO Media, https://www.gzeromedia.com/why-quantum-computing-could-be-a-geopolitical-time-bomb]

What the heck is quantum computing? It's a way of computing that is immeasurably faster than what existing computers do. Traditional computers work by adding up 1s and 0s. Quantum computers are, very roughly speaking, able to make finer distinctions between the two, which allows tremendously complex calculations to be done in a fraction of the time it would take using a traditional computer.

There's still a lot of work left to do before Google, or anyone else, can create a reliable quantum computer that works outside of a narrow laboratory setting, but as this recent article by a computer scientist argues, Google's breakthrough is an important milestone on the way there.

Why it matters: the US, China, Russia, and other countries are racing to roll out national strategies, cultivate talent and pump money into quantum computing. Why? Well, quantum computers have the potential to revolutionize how scientists create new medicines or materials, which could boost health and the national economy. They might even help answer fundamental questions about the nature of the universe, which would be a huge win for science. But much more important than all of that is the fact that whoever can build a powerful enough quantum computer might be able to use it to CRACK ALL OF THE CODES.

Consider: In order to crack the encryption on everything from your bank account to nuclear war plans, today's most powerful supercomputers would have to crunch numbers longer than the lifespan of the known universe. But a powerful enough quantum computer might be able to crack the same code in just a few hours, giving whoever owns it access to other countries and their citizens' most sensitive secrets.

No alarms and no surprises, please: That would be a geopolitical earthquake, and at some point, maybe even soon, it's bound to happen. The big question isn't if, it's how: will it be a surprise when it happens? If so, buckle up. If one country suddenly gained an ability to crack its adversaries' codes it might be tempted to use that power to its advantage, while rivals that suddenly wake up to find their most sensitive information compromised might feel a strong temptation to lash out defensively, heightening the risk of global conflict. A quantum surprise could also have immediate destabilizing effects on the economy if people suddenly feared their money was no longer secure and sparked a run on the banking system.

Conversely, the risks of a major flare-up would be lower if governments and companies were able to give each other some measure of transparency about their quantum projects and to develop new, stronger forms of encryption that can keep pace with that progress to keep essential information secure.

But that doesn't seem to be where things are headed. Instead, technologies like artificial intelligence and 5G have already become hotly politicized by growing strategic competition between the US and China. The closer scientists get to building a working quantum computer, the greater the risk that governments will move the most cutting-edge research behind closed doors. That would heighten the risk that one country or another pops a politically destabilizing quantum surprise.

#### Case-by-case antitrust enforcement fails to address anticompetitive harm produced by restrictive APIs. Only ex ante agency enforcement can adapt to changing market conditions and set norms across industry.

Chao ’20 [Becky; 5/13/20; Fellow in Open Technology Institute @ New America; Former Millennial Public Policy Fellow @ OTI, Former Honors Paralegal in Bureau of Competition @ Federal Trade Commission, BA in Public Policy @ Duke; and Ross Schulman; Senior Counsel and Senior Policy Technologist in Open Technology Institute @ New America, JD @ American University, BS in Computer Science @ Brandeis University; “Promoting Platform Interoperability”; https://www.newamerica.org/oti/reports/promoting-platform-interoperability/]

Platforms Feature Complex Dynamics that Can be Difficult to Address Using Current Antitrust Law

The complex, integrated nature of online platforms makes it challenging to address competition concerns under current antitrust law.29 Digital platforms do not always fit into clear, static market definitions that are foundational to traditional antitrust cases. They also operate in multi-sided markets that antitrust case law may not clearly address.30 The fact that platforms are venturing out into new markets—many of which are rapidly consolidating—adds another layer of complexity for antitrust attorneys and economists to unpack.31 Take, for example, Amazon’s 2017 acquisition of Whole Foods. The FTC cleared the deal and let the parties merge without issuing a second request to conduct a more thorough, formal investigation. The merger between a traditional supermarket and a digital platform with extensive e-commerce operations might have raised difficult questions about defining the relevant market. Many advocates raised concerns that the deal might enhance Amazon’s dominance in fields such as logistics, expand the company’s data trove on consumers, and allow the company to replicate its anticompetitive online tactics in the brick-and-mortar space.32 But it’s not clear that current antitrust law can address these concerns if the merging parties may not appear to directly compete.

The challenge for enforcers is how to measure dominance when the technology, market, and industry are constantly changing. Antitrust agencies must also be empowered with additional resources to improve their capacity for analyzing how market power can be leveraged through data and networks. Further, the case-by-case nature of antitrust enforcement means that even when antitrust interventions are applied, only the specific company involved is obligated to abide by the conditions mandated by the remedy.

Antitrust enforcement operates ex post, meaning that enforcement might only come after the problematic behavior has occurred. Merger review is an exception to this rule, in that enforcers might be able to intervene if the likelihood of anticompetitive harm post-merger is apparent—and even then, merger conditions are often time-limited and the merged entity is not required to abide by them once they’ve expired. Additionally, whether an antitrust enforcer is successful in attaining a desired enforcement action depends on the facts of the specific case, the resources available to bring a case, and, if the enforcers file a lawsuit, the litigation outcome. Ultimately, antitrust enforcement requires a significant time investment, which does not necessarily sync up with the lifecycle of technological innovation and growth. Firms that find themselves excluded from a fair shot at competing—for example, because a dominant platform is engaging in anticompetitive self-preferencing and denying access to its API—might go out of business waiting for the outcome of a case challenging those actions.

Further, structural separation would not remedy all of the competition concerns that online platforms pose.33 Even if a platform is broken up, it could still enter into an anticompetitive arrangement in which only some downstream products are compatible with the platform through proprietary integration or an exclusive contract.

But requirements for interoperability could address some of these threats to competition. As a result, Congress should promote interoperability in new legislation, and the FTC, too, should promote interoperability when appropriate in antitrust enforcement to protect against the anticompetitive risks that arise from dominant platforms’ gatekeeping power.

Platforms Sometimes Inhibit Competition Through API Policy

Interoperability is all the more important when platforms are vertically integrated and, as a result, may have fewer incentives to offer open APIs on their own. Vertically integrated firms offer products that feed into one another along a single production vertical. In the absence of vertical integration, different companies usually produce a different product or service along a supply chain. When firms vertically integrate, however, they usually seek to tap into efficiencies gained from the supply chain integration, and give preference to their own supply chain components when designing products and services to the exclusion of other players in the ecosystem—in their API design, for instance. The more vertically integrated a platform is, the higher the risk that it may not offer APIs with sufficient data and functionality for other companies, particularly downstream businesses, to build products that are compatible with theirs.34 This practice may sometimes threaten competition, but our current antitrust framework insufficiently addresses these risks and does not promote interoperability ex ante (“before the event”).

Vertically integrated platforms have incentives to build their API design solely to their own needs, tailored to their own specific apps, features, and competitive strategy. Twitter, for instance, vertically integrated by purchasing apps like TweetDeck (a social media dashboard application for managing Twitter accounts) in 2011,35 Tweetie (then a leading iPhone Twitter client) in 2010,36 and Summize (a search engine built specifically for indexing Twitter posts) in 2008,37 and as a result was in a position to discourage developers from using Twitter’s APIs to make apps that directly competed with their platform.38 Twitter rejected apps that relied on tweet feed via its API and revoked API access. This practice certainly harmed competition, but may not have been considered anticompetitive within our current antitrust framework because of the challenges in assessing the relevant market, market power, and consumer harm.39

These risks also exist when a platform updates or expands its product offerings.40 For instance, there is a chance that a company may choose to replace older, more open technology with a substitute that is more closed and not conducive to interoperability. A company may also deliberately restrict access to its API as a strategy to deter would-be competitors. Evidence suggests that Facebook has employed this strategy in the past with regards to its API that gave third-party apps the ability to allow users to find and add their Facebook friends on their apps: Facebook turned off its friend-finding API access for Vine (an app owned by Twitter that allowed users to create six-second videos) in 2013 when it began to build out its own video product.41 Facebook said that this policy was geared at cutting off access to its social graph for “apps that [were] using Facebook to either replicate our functionality or bootstrap their growth in a way that create[d] little value for people on Facebook, such as not providing users an easy way to share back to Facebook.”42 The same year, Facebook cut off access to its social graph for MessageMe, a messaging app that had previously been able to allow users to find and add friends from Facebook—just a week after it launched.43 It did the same thing to Voxer, a calling and voice chat communications app that had had access to Facebook’s social graph through its API for over a year before getting cut off.44 It’s worth noting that all three of these competitors ultimately exited the market or shut down—while this loss of competition may be clear, the anticompetitive harm from Facebook restricting its API access in this manner may be more difficult to prove.45

Our current antitrust framework insufficiently addresses the competitive threat of online platforms’ unique gatekeeping ability via control over their own APIs. This practice falls outside of the antitrust theories that have historically addressed similar behaviors from firms: (1) refusal to deal and (2) the essential facilities doctrine.46 Under the former, a monopolist refuses to do business with other firms or prevents customers or suppliers from dealing with the firm’s rivals (i.e., “I refuse to deal with you if you deal with my competitor”) to acquire or maintain its position in the market.47 Under the latter, a monopolist obtains a competitive advantage by denying access to an essential “facility.”48 Neither are entirely applicable to addressing a platform’s control over competitors’ ability to utilize certain aspects of its data and user base to build their own products and services. This distinction is largely because APIs and the underlying data are subject to a variety of other considerations, too, such as the need to protect data security and avoid fraud; these factors require some limitations in the form of access controls and restrictions on usage volume.49 As such, antitrust law is an insufficient tool to address the competitive effects that platforms may raise through their API policies and lack of interoperability.

#### FTC rulemaking on interoperability remedies network effects and facilitates market entry.

Kades & Morton ’20 [Michael Kades and Fiona Morton; Director for markets and competition policy at the Washington Center for Equitable Growth, JD from Wisconsin Law. “Competitive Edge: Remedying monopoly violation by social networks—the role of interoperability and rulemaking”. Washington Center for Equitable Growth. Sept 23 2020. https://equitablegrowth.org/competitive-edge-remedying-monopoly-violation-by-social-networks-the-role-of-interoperability-and-rulemaking/]

All eyes are laser-focused on competition in digital technology platforms such as Amazon.com Inc.’s Marketplace, Apple Inc.’s App store, Facebook Inc.’s eponymous social network, and the search engine operated by Alphabet Inc.’s Google unit. Congress, the Federal Trade Commission, the U.S. Department of Justice, and various state attorneys general are investigating their conduct, and, if press reports are to be believed, both Google and Facebook could soon find themselves as defendants in major monopolization cases. By way of comparison, the previous major monopolization case, United States v. Microsoft, was filed in 1998, when “You’ve got mail,” and that static noise of a dial-up connection were common.

It is, however, past time to think only about whether these technology giants are violating the antitrust laws and ask how to address such antitrust violations if they have occurred. Even in the most successful monopoly prosecutions, such as the antitrust cases against AT&T Inc. in the 1980s and against Microsoft Corp. in the 1990s, the courts struggled to develop and implement effective remedies with various degrees of success. Discussing remedy before there is a case may seem like putting the cart before the horse—but think of it as designing the cart before deciding what horses to use.

Today, we have posted a working paper that proposes a remedy for one type of digital platform: a social network such as Facebook. Our remedy proposal relies on five principles, summarized here and discussed in more detail below:

Social networks, like most digital platforms, have large “network effects.” We discuss this concept in detail below, but the basic idea is that like the telephone system and email, the more people on the same network, the more useful it is to its users. Those network effects create entry barriers, which make it easier for anticompetitive conduct to successfully create and protect monopoly power.

Unless a remedy addresses the entry barriers created by these network effects, it will likely fail to fully restore competition or prevent future violations.

Interoperability refers to the way phones from Verizon Communications Inc., AT&T, and other companies can connect with each other, or users of Gmail and Hotmail can write to each other. In the case of a social network, interoperability would enable social network users on different social networks to seamlessly connect with each other, meaning that interoperability is likely to be critical, although not sufficient, to address harms caused by an antitrust violation.

Implementing interoperability poses challenges for the litigation process. It requires the creation of a technical committee to address the technical details. The committee can’t be manipulated by the dominant players. Policing compliance with the remedy must be efficient. And substantial penalties are needed to deter incentives to violate the remedy order.

The Federal Trade Commission could use its rulemaking authority, outside of any particular litigation, to develop a default interoperability order that could increase the workability and effectiveness of any future interoperability requirement.

Digital platforms are under scrutiny

On Capitol Hill, the Senate Judiciary Committee just held a hearing on Google and online advertising. The House Judiciary Committee will release its report on digital platforms shortly. Jason Furman, a professor of the practice of economic policy at the Harvard Kennedy School and a member of Equitable Growth’s Steering Committee, outlined the role of networks on competition in digital markets in testimony before Congress (available as a Competitive Edge), and Equitable Growth has also summarized research more broadly.

A network effect means a digital platform’s value to users increases as the number of users increases. Take Facebook as an example. As the number of users on Facebook increases overall, any individual will need to be on Facebook to communicate with her friends or family; conversely, no one wants to be on a social network if none of their friends or family use it. Similarly, advertising on Facebook becomes more valuable the bigger Facebook’s user base grows, the longer users are on Facebook, and the more Facebook can help target the ads to those who will most likely respond to them, which is a function of the first two benefits of size.

In turn, this network effect can lead to a winner-take-all (or most) dynamic, also known as tipping. When one social network creates an edge in number of users, either legitimately or through exclusionary conduct, that advantage attracts even more users. The social network may become dominant and earn monopoly returns. Ultimately, the network effect creates an entry barrier. Few will join a new social network until their friends, families, and neighbors do.

Neither entry barriers nor tipping present insurmountable barriers for a new competitor, but they do make it easier to monopolize a market. In a market subject to tipping (even if it is not permanent), the value of excluding a competitor is greater because the prize is bigger. If entry barriers are high, any potential competitor’s chance of success is low. As a result, a social network may be able to inexpensively acquire nascent or potential competitors before they pose a threat to the network’s dominance.

A successful remedy will reduce entry barriers created by network effects

If this type of digital platform has violated antitrust laws, it has engaged in anticompetitive conduct that relies on and exploits the network effect and the entry barriers it creates. Absent intervention, the dominant platform will continue to benefit from its conduct; entry is unlikely and difficult. A divested network can compete with its existing installed base of users, and this will create choice for users—provided their friends move with them. So long as the network effect remains, however, the dominant firm continues to have the same incentives to adopt different and new exclusionary conduct to protect its monopoly. For a remedy to be fully effective, it needs to reduce the network effect and the entry barriers it creates.

Network effects manifest themselves across different types of digital platforms: social networks, online marketplaces, app stores, and online advertising. But they can operate differently in each setting. Network effects can be direct or indirect; platforms can have multiple sides. The effects may be asymmetric, and some may be strong and others weak. A remedy that addresses network effects present in a social network market may be meaningless in addressing network effects in an online marketplace. We use Facebook to explore addressing network effects as a remedy for a monopolization violation involving a social network.

Based on allegations currently being made, assume that Facebook has allegedly acquired a series of nascent or potential competitors to eliminate companies; that it cut off access to Facebook when a company could pose a competitive threat; and that those actions violate the antitrust laws as illegal monopolization. How would one remedy the violation? (Our working paper and this column do not comment on the merits of these allegations.)

Certainly, a court could forbid Facebook from repeating the illegal act and similar acts. Facebook could face fines or have to give up its profits from violating the law. But we are doubtful that those remedies alone would recreate the lost competition and thereby give consumers the competition they were earlier denied. Conduct prohibitions are likely to create an expensive whack-a-mole game, with the government and the dominant firm arguing over both the impact of every new strategy and whether it counts as “similar” to what violated the law.

A more substantial remedy would break up a social network into separate parts and provide real benefits by setting the stage for robust competition. A remedy, for example, could require Facebook to divest its Instagram photo- and video-sharing unit and its messaging unit, WhatsApp. Divestiture would significantly benefit users post-break-up as the divested components would compete with each other to attract users. Each network would innovate and provide better service to win an advantage in the number of users. The competition would likely be fierce. But without additional remedies, the market would likely tip again to one of the competitors, creating another monopoly. Then, the winning social network has both the incentive and ability to engage in exclusionary acts to prevent future threats to its newly established or re-established market dominance.

Interoperability has the potential to lower entry barriers

Requiring interoperability can neutralize or significantly reduce the network effect that the incumbent employed to create and protect its monopoly. By interoperability, we mean that users on other or new social networks should be able to friend Facebook users and vice versa. Posts should flow from a Facebook user to her friend on a new network in much the same way email can be sent and received regardless of whether both parties use Gmail, or phone calls connect people regardless of their carriers.

Interoperability reduces the barriers to entry created by network effects. Let’s say, for example, that one of the divested Facebook companies begins to lose users. It radically changes its business model from advertising-supported to a subscription-based business model and promotes the resulting high-quality user interface. It hopes to attract users because it has no advertising and strong privacy protections. Without interoperability, a user who prefers the subscription model and leaves Facebook to join it will lose contact with all her friends on Facebook and perhaps institutions there, such as her child’s school. Such costs might deter her from joining her preferred network. With interoperability, by contrast, she receives school forms and news of family vacations and college reunions that are sent to her through her new network. In short, with interoperability, each person can choose the network they prefer while staying in touch with their social circles. The network effect ceases to be an entry barrier.

In this world, entering social networks could compete on features outside the standard, such as their user interface, policies concerning news or offensive content, and privacy policies. Consumers could change social networks like they change wireless carriers, without losing the ability to stay in touch with their contacts. The need to compete for consumers on the basis of service quality, such as the amount of advertising and how it is targeted, rather than relying on network effects to keep users, would intensify competition among social networks to the benefit of consumers.

Interoperability could be ordered in addition to other relief, such as a divestiture, and could be complementary to it or stand on its own. It could be an appropriate remedy in any situation in which the dominant social networking firm has exploited network effects by violating antitrust laws. In today’s internet-based network markets, interoperability carries no incremental costs such as the dedicated wires and machines that were required for telecom interoperability in past decades. It requires the establishment of an open standard to exchange commonly used functionalities, such as text, calendars, and images between and among competing social networks.

The challenges of implementing interoperability as a remedy

Although interoperability as a concept is straightforward, effectively implementing it raises challenges. In our working paper, we look back at both the AT&T break-up order, where interoperability was effective, and the remedial order in United States v. Microsoft, where those provisions had little impact. From those cases, we suggest several operational principles.

Substantively, the remedy must establish the technical capability for users to communicate across platforms, balance the needs of multiple actors, promote entry, and enhance the user experience, including protecting privacy. Importantly, the remedy order must prevent the offending, dominant social network (or its divested parts) from manipulating the process. This requires that the remedy include provisions that will deter the defendant from violating the order, require standards that many entrants can meet, and not favor large incumbents.

The remedy also must establish a process for determining whether the defendant has violated the order. That process must be fast enough to provide relief to a harmed competitor before that firm fails, and the penalties must be significant enough that the dominant social network will be worse-off for having violated the remedy order.

From a process perspective, creating a technical committee overseen by an antitrust enforcer is the most promising option to solve these implementation challenges. Judge Harold Green used a similar procedure in the AT&T break-up, and Judge Colleen Kollar-Kotelly relied on a technical committee in Microsoft. Such a committee would include representatives of all relevant industry segments, but the antitrust enforcer engaged in policing the remedy would control the decision-making process to prevent capture by the dominant social network (or its divested parts).

FTC rulemaking can improve the remedy process

The final element of our proposal is that the Federal Trade Commission should use its rulemaking authority to develop a default order for interoperability. Rulemaking provides a number of advantages for developing the groundwork for a successful remedy. A default order derived through rulemaking can identify basic principles to apply in monopolization cases involving strong network effects or issue separate rules on remedies for different types of digital platforms.

In an administrative adjudication, where the Federal Trade Commissioners are the judges, the default order would be a mandatory starting point for a remedy. In cases brought in federal court by the Justice Department’s Antitrust Division, the states, or the Federal Trade Commission (the FTC can either bring cases internally, where it acts as a decisionmaker, or in federal court, where it is the plaintiff), courts would not be required to rely on the default order but would be free to do so.

In any individual case, the decision-maker could adjust the terms as necessary to fit the particular situation, but the default order would save time and effort. The default order would also help focus on the issues in dispute. Parties could appeal any of the decisions we describe to the courts. Given the existence of a carefully crafted, robust order, however, those appeals would likely be less frequent and burdensome than if a court had to resolve every issue from scratch.

Conclusion

The debate over whether any digital platform violates antitrust laws will continue in the press, in the halls of Congress, and, probably, in courtrooms across the country. Antitrust policymakers need not—and should not—wait for a liability determination before considering remedies they can apply today, using current law and existing institutions. Our working paper provides a contribution to the remedy discussion and on the need to address entry barriers as a necessary, but not necessarily a sufficient, goal of a successful remedy.

#### Ex-ante mandates are key.

Cyphers ’21 [Bennett; and Cory Doctorow; Staff Technologist on the Tech Projects team. Special consultant to the Electronic Frontier Foundation, MIT Media Lab Research Affiliate, visiting professor of computer science at the Open University, visiting professor of practice at the University of North Carolina’s School of Library and Information Science, co-founder of the Open Rights Group. “Privacy Without Monopoly: Data Protection and Interoperability”. EFF. Feb 12 2021. https://www.eff.org/wp/interoperability-and-privacy]

3.2. Interoperability Mandates1

The second part of our proposal is a new set of legislative and administrative mandates for specific flavors of interoperability. These mandates are designed to force platforms to open up key parts of their infrastructure to help alleviate the network effects that keep competitors from getting a foothold.

Our proposals are based on the framework laid out in the ACCESS Act of 2019. Legislation is one possible tool for implementing these policies, though they may also be implemented by other means, such as consent decrees or voluntary covenants. We recommend that any new mandates define the behaviors that businesses must support, but not the specific ways they should do it. And while protecting innovation in general is important, regulators and lawmakers must be extremely careful not to hamper companies’ ability to react to new security vulnerabilities or privacy threats.

We endorse new mandates in three areas: data portability, back-end interoperability, and delegability. Together, these give users the power to use platforms on their terms, and allow competitors to use incumbent platforms to launch new, innovative rivals.

Back-end interoperability and delegability mandates are designed to tip the scales away from entrenched platforms and towards smaller competitors, so we recommend that, at least at first, these should only apply to the largest monopolists. On the other hand, portability is a tool for both interoperability and user empowerment, so it should apply to a much wider range of companies.

3.2.1. Data portability

The first and simplest new policy is a universal right of data portability. Users deserve to do what they want with their data, and should have a right to quickly, easily download or move the data that a platform has about them. Compared to the other ideas in this paper, data portability is a relatively easy policy lift: laws have already created partial or full data portability mandates in several jurisdictions. The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) both include some form of data portability mandate; as a result, most companies that do business in either California or Europe already have portability processes in place.

Portability is as much about user rights as it is about interoperability between businesses. Therefore, the scope of a portability mandate should be wide. Most companies that collect or process users’ data should be required to make that data portable. Portability should also be less of a technical lift than the other mandates we discuss below.

Although the central idea of portability mandates is simple to grasp—that users should be able to access their data in a useful, accessible form—companies have clashed with regulators over just what data should be portable. Incumbents have argued that some data implicating other users is too sensitive to allow for simple porting. Conveniently, that “too sensitive” data is often the same data, such as friends’ contact information, that is key to helping small competitors off the ground.

Still, large platforms now generally agree that portability mandates are acceptable, even beneficial. Google, Microsoft, Facebook, and Twitter are among the founding partners of the Data Transfer Project, an attempt to develop secure standards for sending user data from one service to another. Last year, Facebook signaled support for the portability mandate proposed in the ACCESS Act, and requested that regulators tell companies exactly what they need to export.

Who has a right to what data? And what should they have a right to do with it? Those questions are central to getting a portability mandate right.

3.2.2. Back-end interoperability

The second flavor of mandate is back-end interoperability, which has a much more extensive set of requirements. The goal of this kind of mandate is to allow users of small services to interact with users on big platforms. This gets directly at the network effects that make it so easy for Facebook and YouTube to shrug off competition.

A back-end interoperability mandate would require platforms to allow competitors to work with their internal systems on behalf of users whose data lives elsewhere. The core principle of the mandate would be this: any service operated by the platform that allows users to communicate with each other—whether by direct message, public or semi-public posts, comments, or reactions—should allow users that are not signed up with the service to engage in those same kinds of communication.

Think about what it would mean to interact with Facebook as a user of a similar, but distinct, social network. For full, meaningful interoperability, you’d need to be able to read, comment on, and react to content on Facebook in such a way that Facebook users can actually see it. You’d need Facebook to treat you in the same way that it treats its own users, but without controlling the authentication or data storage for your account. Broadly, this would require Facebook to create new connections in two directions: first, it would need to share data from its own users with third-party services; and second, it would need to ingest data from users of those outside services. (Example 2 explores this scenario further.)

This kind of requirement may be burdensome to the companies that are subject to it. Therefore we recommend that, at least at first, these should only apply to dominant platforms that can afford the new costs of compliance. Furthermore, we recommend that policymakers stay away from being overly prescriptive wherever possible—as long as platforms build tools that make the desired data flows possible, and as long as there are appropriate safeguards for user privacy, it should not matter how they do it. This will leave room for future optimization and innovation.

This kind of rule will be hard to do right, and will require ongoing monitoring. Regardless, it is worth doing.

Example 2: Federated social networking

If we break Facebook’s monopoly power in social networking, what comes next? How would we go about breaking that monopoly power in the first place? The answer to both questions could be the same: a truly federated social network, in which users who have signed up for different services can interact with one another freely. To get there, Facebook would need to allow its users to become “friends” with accounts hosted on rival services.

Facebook already has APIs that allows developers to access pretty much all data on behalf of a Facebook user. This lets developers build add-ons to Facebook’s core product, or glue between a user’s Facebook account and their account on another service. But it doesn’t allow developers to access data on behalf of users who are not on Facebook at all.

To federate, Facebook would need to create an interface to allow Facebook users to become friends with off-platform identities. Facebook would have to explain to its users the kinds of data it will be sharing, and with whom. The user must trust at least two different actors: first, the administrator of the service they will be sharing data with, and second, whomever they are trying to connect with on that service. The user must also have an easy way to opt out of sharing data with either or both of those actors at any time. That means a way to “un-friend” the user on the other service, as well as a way to cut off the other service’s access to their data altogether.

On the back end, Facebook would have to set up interfaces for bi-directional data flow between itself and third-party services. Its Graph API already provides (or has in the past) most of what’s needed for moving data out of Facebook: apps can already get programmatic access to a user’s posts, likes, photos, and basic profile information.

The third-party service also needs a way to push data into Facebook. This means Facebook has to consume content from third-party users and distribute that content appropriately. It could accomplish this by letting outside services push updates that are shaped like Facebook data—posts, comments, and reactions—on behalf of their own users. Facebook could then display that content to its users in their regular feeds.

Together, these pieces would change Facebook from a social media pocket universe, where users may only communicate with others inside the system, into a single part of a constellation of social networks. People who are already invested in Facebook—that is, most of us—could try out new services without leaving all their old connections behind.

All of this is unlikely to happen without outside incentive; it is simply not in Facebook’s interests to interoperate with potential competitors. It is more likely that Facebook will only adopt strong interoperability as a result of a legal mandate—or as part of a deal to avoid more dire consequences, like structural separation. Legal mandates—namely, for back-end interoperability—would need to outline what functionality Facebook needs to support, and govern how the company is allowed to moderate access to its new interfaces.

3.2.3. Delegability

The third kind of mandate is delegability, or client-side interoperability. The concept is simple: anything you can do with a mouse or a touch screen to interact with a platform, you should be able to delegate to someone’s code to do on your behalf. Every substantial part of the user interface should be available to automated access. This means that a user could delegate a piece of software—either their own, or a trusted third-party tool—to interact with a platform on their behalf. These “delegated agents” will be able to tip the balance of power between users and platforms so that users come out on top.

Delegability is closely related to ComCom. With a robust competitive compatibility regime, developers would be free to try to build on top of existing user interfaces. Delegability would take this to the next level, and guarantee that developers have stable, usable programmatic interface to act on behalf of users.

Delegability is new to the tech sector, but it’s been pioneered in other industries through right-to-repair laws. Right-to-repair laws generally seek to mandate that manufacturers provide necessary repair and diagnostic information and parts to independent service providers and, sometimes, device owners. Some also go further, such as Massachusetts’ requirement that cars use a standardized interface for pulling diagnostics and communicating with on-board computers. Automotive right-to-repair laws have helped open up huge secondary markets for independent diagnostics, repair, and engine tuning.

A delegability mandate can provide the benefits of client-side APIs without the risk of arbitrary moderation or sudden rollbacks that platforms have historically imposed. This kind of mandate could open space for a whole host of new user-friendly applications, from custom filters on social media feeds to new tools for accessibility, from audits of political ads to independent stewardship of privacy settings. This kind of mandate guarantees that platform interfaces will remain stable and accessible, making it more feasible for users and developers to invest in building on them.

Example 3: Third-party privacy controls

Many sites offer relatively detailed privacy settings. Facebook has several different pages that control data collection, sharing, and use across a suite of (sometimes linked) products. And these settings’ defaults and options change over time, often without notice. Users generally do not want to think about every single setting; many would prefer to have the most privacy-preserving settings turned on by default. An “install-and-forget” privacy setting app would allow users to delegate an intermediary to make sure they are getting the most private experience possible over time.

Competitive Compatibility would make this possible. A browser extension designed around the particular workings of platforms’ privacy pages could automatically load up the page, set the preferred check boxes and sliders, and warn the user when companies deploy dark patterns to get them to “opt back in.”

In a ComCom-based solution, tools would be fragile, and subject to Facebook’s decisions to fight them off. If the company wanted to fight with interoperators, it could deploy many of the same tools it does against ad-blockers and ad fraud networks. That would lead to a technical back-and-forth, with some tools able to stay ahead of Facebook’s maneuvering, and others breaking as they fall behind. In a ComCom world (where Facebook no longer has legal remedies against interoperators) Facebook might arrive at an equilibrium where it offers privacy tools a managed access—or Facebook might decide to fight on, judging that the anger of users who are kicked off of Facebook for violating its terms of service is a price worth paying for continued dominance.

Delegability would set in stone the right to outsource privacy decisions. A delegability mandate guarantees users a right to programmatically interoperate, and Facebook would defy users at its own legal peril. A privacy setting tool isn’t merely possible, it’s simple. It could be integrated into tracker blockers and even browsers themselves. Users could install a pan-platform privacy toolkit to keep them protected across all entities subject to the mandate.

The obvious privacy risk with this kind of tool is that the delegated agent could turn out to be a bad steward of user privacy. But because the tool would be so easy to build, it could be volunteer-developed free software. Users could choose a tool from an actor they trust not to have ulterior motives.

#### Certainty and federal action are key – a thicket of legal defenses discourages interoperating.

Doctorow ’21 [Cory; 4/13/21; Special Consultant @ Electronic Frontier Foundation, Research Affiliate @ MIT Media Lab, Visiting Professor of Computer Science @ Open University, Visiting Professor of Practice in School of Library and Information Science @ University of North Carolina, Co-Founder @ Open Rights Group; “Unfair Use: Anti-Interoperability and Our Dwindling Digital Freedom”; <https://thereboot.com/unfair-use-anti-interoperability-and-our-dwindling-digital-freedom/>; \*GPL = General Public License, “a copyright license for computer programmers who want to share their work”]

Some 40 years later, the world is a very different place. Between software copyrights, anti-circumvention rules, software patents, enforceable terms of service, trade secrecy, noncompete agreements, and the Oracle/Google dispute over API copyrights, any attempt to interoperate with an existing product service without permission from its corporate master is a legal suicide mission, an invitation to almost unlimited civil — and even criminal — litigation. That is to say: if you dare to modify, improve, or replace an existing, dominant software-based product or service, you risk bankruptcy and a long prison sentence.

Forty years ago, we had cake and asked for icing on top of it. Today, all we have left is the icing, and we’ve forgotten that the cake was ever there. If code isn’t licensed as “free,” you’d best leave it alone.

\* \* \*

What is “interoperability,” anyway?

The term is nerdy, technical, obscure. It’s closely related to the slightly more familiar “compatibility,” but the two aren’t quite equivalent. In a technical sense, “interoperability” describes two products or services that can somehow work together with one another. From opening your Microsoft Word documents in Google Docs, to using third-party ink cartridges in your printer, to replacing your watch band, to changing the stereo that came with your car, interoperability is a broad, universal, essential characteristic of all of our technology.

Interoperability is the default state of the world. Anyone’s charcoal will burn in your barbecue, just as anyone’s gas will make your car go. Any manufacturer can make a light bulb that fits in your light socket, and any shoes can be worn with any socks. Some of this is down to standardization: manufacturers, academics, regulators, and interested parties gather in “standards development organizations” to make this process simpler, describing the canonical direction and spacing of a light bulb thread, or the syntax of an HTTP request, or the fittings on the underside of your toilet.

This certainly makes interoperability smoother! Standards for paper, from weight (grams per square meter, or GSM) to size (letter/legal/tabloid; A1, A2, A3, A4, etc.) make it possible for you to reliably buy paper that will work with your printer without requiring additional trimming or other modifications.

A failure to standardize can make life hard for everyone. Early Australian rail barons laid their tracks in several gauges, leading to the “multi-gauge muddle” of a rail system where some cars and engines could not run on some of the tracks.

These barriers to interoperability aren’t insurmountable. If your paper doesn’t fit your envelope, you can fold it; if it doesn’t fit your printer, you can trim it. If the rail gauge doesn’t match your rolling stock, you can modify the undercarriages to allow for multi-gauge operation (a difficult operation to be sure, never implemented despite hundreds of proposals) or you can tear up some of the track and lay new ones (as Australia has done and promises to do more of).

Interoperability lowers “switching costs” — the cost of leaving behind whatever you’re using now in favor of something you think will suit you better. When my grandparents emigrated to Canada from the Soviet Union on a displaced persons ship, they incurred a high switching cost. For more than a decade, they had no contact with their family in Leningrad except through unreliable, slow word of mouth with the rare person who got a visa to travel there.

Contrast this with my move from the UK to Los Angeles in 2015. We are in routine contact with my in-laws in London and Wales, as well as my family in Toronto. My laptop and books came with me, as did our other personal effects. We left most of our appliances behind because they ran on a different voltage, but there were a few things we loved that we brought with and either changed the plugs on or connected to our house’s electrical outlets via transformer or adapters.

Companies like high switching costs. For a would-be monopolist, the best product is one that’s seductively easy to start using and incredibly hard to get rid of. Think of Purdue Pharma’s gleeful internal memos — revealed in leaks and court cases — about the ease with which their “customers” were getting started on opioids, and their contempt for how hard it was for those same people to switch away.

Addiction isn’t the only way to raise switching costs. Facebook makes it incredibly easy for you to get started, historically going so far as to tricking you into giving it access to your electronic contacts list to enmesh you in a network of others who have already signed up for the service. Once you’re on Facebook, it’s very easy to bring in articles from the public web and to link to your friends’ updates on rival networks. You can start by just using Facebook to follow the friends you have there, but over time, the system nudges you toward using Facebook as your primary means of reading the news and even following what your friends are saying on non-Facebook networks.

But when you want to leave Facebook, there’s no easy way to do so. You can’t go to a Facebook rival and follow what your friends post to Facebook from there. You certainly can’t reply to what your Facebook friends post using a rival service.

Interoperability — the thing Facebook uses to slurp stuff in from the open web — is the key to self-determination. Leaving Facebook in the 21st century is like my grandmother leaving the USSR in the 40s. You can go, but your friends and loved ones are all held hostage behind Zuckerberg’s Iron Curtain, so leaving Facebook means leaving your communities, your relationships. That’s not as hard as kicking opioids, but it’s not easy either. And your presence on Facebook is the reason someone else can’t go.

Here’s the thing: everyone wants to minimize risk, from employers to workers, from Big Tech to its users. You want to use Google in ways that make your life better, and you don’t want Google to be able to arbitrarily change or remove the services it provides. (Ask me how bitter I am about Google nuking Reader, its RSS product!) Google wants to ensure that you won’t leave the company or its products and services. It could improve its retention by making you so delighted with its offerings that you’d never consider leaving. But a surer, cheaper way is to interweave its products and services with your life: making sure that your kid can’t go to a public school without creating a Google account; embedding Google search in your mobile OS; releasing web- and app-development frameworks for third parties that quietly harvest the data of their users and send them to Google; etc.

The more freedom you have to leave Google, the bigger a risk you present to Google. The more Google can lock you in, the lower the risk of your departure from the service — and the higher the risk that Google will cease to keep your business by making good products, and instead rely on retaining you because you can’t leave (or because leaving comes at a very high price).

Interoperability improves self-determination by safeguarding your ability to change the current situation by incremental steps. If you like your phone and the apps you have but want an app that’s banned in its default app store, interoperability comes to the rescue, allowing you to add a second app store to your phone’s list of approved software sources. You get to keep your phone, keep your apps, keep all the data on your phone, and you get to install that unauthorized app.

Without interoperability, your choice is “take it or leave it.” If the app store blocks an app you want, the price of getting that app is throwing away your phone, all its apps, and some or all of the data you’ve painstakingly input into your phone. That unauthorized app needs to be pretty darned good before anyone would pay such a high price for it.

Writ large, interoperability encompasses things like democracy. When someone says they like their city but not its bylaws, we don’t tell them that the law is the law and the home comes with these bylaws in a package. Instead, we set out processes for amending or repealing laws that chafe the people they govern. If you fail in your bid to reform your city’s laws, you can also move to another city without having to surrender the possessions in your home or your social relations with your old neighbors. Interoperability lets you replace the laws and keep your house, or replace your house and find new laws.

\* \* \*

This whole line of thought started with a reflection of the history of the free software movement: the largely forgotten time in which the default condition of software was freedom. In the absence of copyright, patent, anti-circumvention, terms of service, noncompetes, confidentiality, and other commonplaces of today’s software marketplace, anyone who could figure out how to reverse engineer a program could improve it, replace some or all of it, read or write its files, compete with it, or sideline it.

Today, this is no longer the case. In fact, today’s software marketplace is so unlike our previous “cake-and-icing” world — where the default was software freedom (cake) and the free software movement began its audacious demand for freely reusable source code as a means of making software freedom as frictionless as possible (icing) — that it’s virtually impossible to imagine such an environment.

The thicket of anti-interoperability rules that has sprung up around interoperability has a catch-all name: “intellectual property.” Now, free software advocates — and free culture advocates — hate the term “intellectual property.” The argument against IP rails against its imprecision and its rhetorical dishonesty.

Prior to the rise of “intellectual property” as an umbrella term, the different legal regimes it refers to were customarily referred to by their individual names. When you were talking about patents, you said “patents,” and when you were talking about copyrights, you said “copyrights.” Bunching together copyrights and trademarks and patents and other rules wasn’t particularly useful, since these are all very different legal regimes. On those rare instances in which all of these laws were grouped together, the usual term for them was “creator’s monopolies” or “author’s monopolies.”

The anti-IP argument leans into the differences between the underlying rationale for each of these rules:

US copyrights exist to “promote the useful arts and sciences” (as set out in the US Constitution); that is, to provide an incentive to the creation of new works of art: copyright should offer enough protection to create these incentives, but no more. Copyright does not extend to “ideas” and only protects “expressions of ideas.”

Patents exist as incentive for inventors to reveal the workings of their inventions; to receive a patent, you must provide the patent office with a functional description of your invention, which is then published. Even though others may not copy your invention during the patent period, they can study your patent filings and use them to figure out how to do the same thing in different ways, or how to make an interoperable add-on to your invention.

Trademarks exist as consumer protection: trademarks empower manufacturers to punish rivals who misleadingly market competing products or services that are likely to cause confusion among their customers. It’s not about giving Coca-Cola the exclusive right to use the work “Coke” — it’s about deputizing Coca-Cola to punish crooks who trick Coke drinkers into buying knockoffs. Coke’s trademark rights don’t cover non-deceptive, non-confusing uses of its marks, even if these uses harm Coca-Cola, because they do not harm Coke drinkers.

Seen in this light, “intellectual property” is an incoherent category. When you assert that your work has “intellectual property” protection, do you mean that you can sue rivals to protect your customers from deception; or that the government will block rivals if you disclose the inner workings of your machines; or that you have been given just enough (but no more) incentive to publish your expressions of your ideas, with the understanding that the ideas themselves are fair game?

When you look at how “IP” is used by firms, a very precise — albeit colloquial — meaning emerges: “IP is any law that I can invoke that allows me to control the conduct of my competitors, critics, and customers.”

That is, in a world of uncertainty, where other people’s unpredictability can erode your profits, mire you in scandal, or even tank your business, “IP” is a means of forcing other people to arrange their affairs to suit your needs, even if that undermines their own needs.

There are some ways in which this is absolutely undeniable. Take digital rights management, or DRM. These are the digital locks in our devices that prevent us from using them in ways that the manufacturer dislikes. Your printer uses DRM to force you to buy ink that the manufacturer has approved; your phone uses DRM to force you to buy apps that the manufacturer has approved. Ventilators from Medtronic and tractors from John Deere use DRM to force you to get them repaired by the manufacturer — and to scrap them when the manufacturer decides it’s time for you to buy a new one.

Copyright laws — that is, “IP laws” — ban tampering with DRM, making it a serious, jailable felony to provide others with tools to bypass DRM. From Section 1201 of the US Digital Millennium Copyright Act to Canada’s Bill C-32 to Article 6 of the EU Copyright Directive, countries around the world have imposed indiscriminate bans on breaking DRM.

These are all copyright laws but, tellingly, the ban on breaking DRM is not limited to copyright infringement. Bypassing DRM to get your printer to accept third-party ink is not a copyright violation: you’re not reproducing its code, nor are you duplicating the traces etched into its chips. But even though you’re not breaking copyright when you jailbreak your phone, you’re still breaking copyright law. The law bans legal conduct, if you have to break DRM to engage in it. This isn’t copyright protection — it’s felony contempt of business-model.

It’s not just DRM. Take “Goldman Sans,” a free font released by the finance giant and global supervillain Goldman Sachs. Goldman Sans is a copyrighted work, and it comes with a copyright license that you “agree” to when you download the font. Among the license terms for Goldman Sans is a non-disparagement clause — that is, a clause that prohibits you from using the font to criticize Goldman Sachs. Goldman Sachs doesn’t need copyright law to prevent people from copying its font. It gives the font away for free. Goldman Sachs needs copyright law so it can boss people around — so it can tell them what they may (and may not) say.

The risks to free expression and self-determination have always been latent in copyright, patent, and trademark laws, and these laws have historically been designed to minimize those risks. Each one has its own “escape valve” that, theoretically, stops “IP owners” from using their rights to take away your rights.

Copyright has “fair use” (“fair dealing,” in most non-US English-speaking countries), which allows for many kinds of copying, adapting, displaying, and even selling of others’ copyrighted expressions, provided that these activities promote a free and robust discourse by transforming, commenting on, or analyzing the copyrighted work. Fair use doesn’t depend on a copyright holder’s permission — you can make fair uses even (especially!) if the rights holder doesn’t want you to.

Patent has its own escape valve: publication. To receive a patent, you must disclose how your invention works, and those disclosures are on display from the start, where anyone can study them and use them as inspiration for their own inventions. Patents allow you to punish people who duplicate your invention, but they also require that you tell people exactly what steps they must take to effect such a duplication, and also provides a roadmap for replicating your invention’s functions without violating your patent.

Trademark has two important escape valves. First, trademark holders are limited to enforcing their marks against rivals who use them in deceptive ways likely to cause public confusion. Second, trademark is subject to the “nominative defense” — it’s not a violation of a trademark to use that mark to describe the goods or services it’s associated with. You can put a sign in your shop window reading, “We fix iPhones” or “Cheap ink for HP printers” or “Our cola tastes better than Coke!” and there is nothing the trademark holder can do about it.

These escape valves have been a lot less durable than we might have hoped. It turns out that much of their efficacy depends on there being robust competition in the marketplace, so that when one company tries to narrow, say, fair use in court, other companies that depend on fair use spring up to defend it. Through the past four decades of massive consolidation in every industry, a consensus has emerged among the shareholder and managerial classes that these escape valves are defects in otherwise excellent laws, and they have set to work creating legal precedents, new laws, and new legal tactics to jam these valves shut.

\* \* \*

This is how we went from having software freedom cake to just having the icing: new copyright laws (like the ones that ban breaking DRM); new copyright precedents (like the one Oracle just failed to win in its lawsuit against Google); and new tactics for combining copyrights, patents, trademarks, DRM, trade secrets, and other IP so that what trademark permits, copyright prohibits, and what copyright permits, patent blocks, and so on — until all the certainty has been moved onto the manufacturer’s side of the deal, and all the risk has been moved onto yours.

#### Gene sequencing database interoperability metagenomic microbiodiversity sequencing.

Ellisman ’17 [Mark; UC San Diego/National Science Foundation; “EAGER: An Interoperable Information Infrastructure for Biodiversity Research (I3BR),” https://www.nsf.gov/awardsearch/showAward?AWD\_ID=1255035]

Biodiversity comprises all variations of life at all levels of biological organization, most of which arise from genomic diversity. As genomic technologies become available across the biological sciences, a full characterization of biodiversity demands a full characterization of genomes. Similarly, data synthesis across the full range of biodiversity research domains demands development, implementation, integration and harmonization of data exchange standards. Such interoperable informatics would be transformational for our understanding of biology, with consequent impact on environmental and conservation policy. Adding to the transformational potential is the fact that the microbial world represents half of the world's biomass and nearly all of its biodiversity, yet is still effectively invisible and intractable to traditional biodiversity research. Metagenomic data are not amenable to the concepts, standards, semantics, and methods of traditional eukaryotic biodiversity, and therefore, require an alternate informatics framework. The EAGER will transform the collaborations between two previously separate research communities: the informaticists of the traditional biodiversity community, who employ the Darwin Core (DwC) as a standard, and the informaticists of the Genomic Standards Consortium (GSC), who have developed the Minimal Information about any Sequence (MIxS) standard for genomics, metagenomics and marker genes. Together, these groups will engage in a unified informatics effort to develop three layers of interoperability. The EAGER will harmonize the observational (DwC) and genomic (MIxS) standards, building on a community dialogue and interdisciplinary networking hosted and established under an NSF Research Coordination Network. Standards interoperability is the basis for the next two layers. Syntactic interoperability (in the context of Internet APIs and a database Reference Model) will be supported. The EAGER will assemble experts from the two communities to (a) devise a database Reference Model that integrates the DwC and GSC MIxS standards; and (b) for effective data management, create specific implementations for different database platforms to foster adoption. The practical implementation of the reference model on/for different database systems will allow, for the first time, systematic comparative testing of technical performance and of use cases (e.g., which implementation best serves which complex data query). The EAGER will create task groups to establish the infrastructure for managing ontologies, and to construct a reference model on the purely semantic level in order to fuse the two worlds of data standards, both of which are advanced enough to engage in useful interoperability. In developing an interdisciplinary information infrastructure to achieve data interoperability across domains, this EAGER would advance understanding of complex environmental phenomena and, thereby, inform future policy decisions. Indeed, by leading to an informatics standards platform to conceive a novel conceptual and theoretical framework for the world of microbial ?dark matter,? the EAGER would have a transformational impact beyond science.

#### Microbial biodiversity solves extinction.

Sharma ’22 [Sunanda, Chair of Applied and Molecular Microbiology @ Technische Universität Berlin, and Vera Meyer, Microbio @ Technische Universität Berlin; “The colors of life: an interdisciplinary artist-in-residence project to research fungal pigments as a gateway to empathy and understanding of microbial life” Fungal Biol Biotechnol. 2022; 9: 1. Published online 2022 Jan 10. doi: 10.1186/s40694-021-00130-7]

The limited discovery and quantification of microbial diversity is a significant challenge to our understanding of the biodiversity of Earth. A great deal of life on our planet may in fact be microbial, yet we are estimated to know less than 1% of existing microbial species [2] and little to nothing about the trends regarding its diversity and rate of change [3]. Even the microbial species we know of, including many bacteria, fungi, archaea, and protists, are often understudied. This may be in part due to the fact that they are individually difficult or impossible to discern with the naked eye, limiting observation and interaction by humans. The mismatch of physical scale between microorganisms and humans has been proposed as the reason for a “size bias” against microbial life, resulting in their exclusion from the ethical frameworks utilized in laboratory research [4, 5]. In addition, microorganisms lack key features that humans have been shown to have strong affective and empathetic responses to, such as visible neotenic characteristics, similarity to human appearance, the possibility of communication, and aesthetic beauty [6]. Furthermore, research on human empathy for other organisms indicates that there is an inverse relationship between empathy inspired by the species and evolutionary divergence time, suggesting that achieving human empathy for microorganisms is a challenging endeavor [7]. Yet, it is well accepted that microorganisms are essential to agriculture [8], major biogeochemical cycles [9, 10], and the evolution of higher life forms [11, 12]. In addition, they are ubiquitous in and on the human body [13] and built environment [14, 15], so may be deserving of unique ethical consideration. Microbial diversity is fundamental to not only the maintenance of global resources and, in turn, human survival [16, 17], but microorganisms are now being increasingly pursued for their potential in biotechnological applications such as the production of biopharmaceuticals [18], and use in bioremediation [19, 20]. Given that human preference directly affects the success of preservation and conservation efforts [21], it is critical that microbes are reconsidered in an empathetic light if their survival and diversity are to be maintained. Approaches for increasing human empathy for non-human organisms have been explored most widely in the field of conservation biology and can be grouped into five themes: promoting anthropomorphism, demonstrating utility, eliciting emotion (such as sympathy, protectiveness, or curiosity), promoting practical engagement, and attachment to nature, and highlighting aesthetic beauty. The first approach focuses on finding or creating similarities between a target species and humans to develop empathy, such as by adding human-like faces onto representations of animals; it has more recently been refined in an attempt to reduce anthropocentric bias [22]. The second approach focuses on examining and communicating the usefulness of a target species to human survival or daily life. For instance, public interest in insect pollinators has been sought by presenting data on their widespread positive effect on globally important crops as well as quantifying their service contribution to market output [23]. The third approach has similarly been used to call for support for pollinators such as honeybees (Apis mellifera) by describing their plight and the potential role of humans as protectors [24]. The fourth approach has been explored through citizen science efforts to engage the public in the research and conservation of various organisms such as native North American songbirds [25], butterflies [26], and bumblebees [27]. Finally, highlighting aesthetic beauty has been used effectively to promote interest in some organisms, such as butterflies [28].

### 1AC – Plan

#### The United States federal government should establish the standard of digital platform interoperability.

### 1AC – Middleware

#### Advantage two: Middleware

#### Platforms’ power over information collapses democracy and ensures spread of misinformation – clickbait and inflammatory content spread because they sell.

Fukuyama ’21 [Francis; Mosbacher Director @ Stanford’s Center on Democracy, Development and the Rule of Law; “Making the Internet Safe for Democracy,” *Journal of Democracy*, 32(2), p. 37-44]

Many people have come to see the internet as one of the chief threats to contemporary democracy. The internet, and large platforms such as Google, Facebook, and Twitter in particular, have been blamed for the rise of Donald Trump and the populism he represents, the proliferation of conspiracy theories and fake news, and the intense political polarization afflicting the United States as well as many other democracies. Across the world, politicians with authoritarian leanings, such as Rodrigo Duterte in the Philippines and Narendra Modi in India, have made effective use of Facebook and Twitter to reach their followers and attack opponents.

There is, nonetheless, a great deal of confusion as to where the real threat to democracy lies. This confusion begins with a question of causality: Do the platforms simply reflect existing political and social conflicts, or are they actually the cause of such conflicts? The answer to that question will in turn be key to finding the appropriate remedies.

This issue came to a head in the aftermath of the 6 January 2021 mob assault on the U.S. Congress that was instigated by the outgoing President Trump. In the wake of that violence, Twitter shut down Trump’s account, cutting him off from the primary channel that he had used to communicate with his followers. While many people applauded this decision and even saw it as overdue, others worried about the sheer power that Twitter had amassed. President Trump was indeed effectively muzzled in the days following the ban. Conservatives immediately castigated the move—and the parallel actions by Facebook, Google, and Amazon that soon followed—for what they labeled “censorship.” And while one may approve of Twitter’s decision as a short-run response to the danger of violent incitement, conservative critics of this move raise legitimate points about the dangers of platform power.

Legally speaking, the censorship charge falls flat. In U.S. law, the First Amendment’s prohibition of censorship applies only to government actions; the Amendment actually protects the right of private parties such as Twitter and Facebook to publish whatever content they want. Beyond these protections, online platforms have been shielded from certain forms of liability by Section 230 of the 1996 Communications Decency Act. The problem we face today, however, is one of scale: These platforms are so large that they have come to constitute a “public square” within which citizens contest issues and ideas. There are plenty of private corporations that curate the information they publish; these are media companies, with names such as the New York Times or the Wall Street Journal. But none of these legacy media companies is as dominant or reaches as many people as Twitter, Facebook, and Google. The scale of these internet platforms is great enough that decisions made by their owners could impact the outcome of democratic elections in a way that legacy media companies� decisions could not.

The other big problem with the large internet platforms is one of transparency. While Twitter publicly announced its ban of President Trump, it, Facebook, and Google make literally thousands of content-curation decisions each day. The great mass of takedowns are relatively uncontroversial, as with those targeting terrorist incitement, child pornography, or overt criminal conspiracies. But some decisions to flag or remove posts have been either more contentious or simply erroneous, particularly since the platforms began to rely increasingly on artificial-intelligence (AI) systems to moderate content during the covid-19 pandemic. An even more central question concerns not what content social-media platforms remove, but rather what they display. From among the vast number of posts made on Twitter or Facebook, the content we actually see in our feeds is selected by complex AI algorithms that are designed primarily not to protect democratic values, but to maximize corporate revenues. It is thus unsurprising that these platforms have been blamed for propagating conspiracy theories, slander, and other toxic forms of viral content: This is what sells. Users do not know why they are seeing what they see on their feeds, or what they are not seeing because of the decisions of an invisible AI program.

Harms

We thus need to be precise about the nature of the threat that the large platforms pose to modern liberal democracy. It does not lie in the mere fact that they carry “fake news” or conspiracy theories or other kinds of harmful political content. The U.S. First Amendment protects the right of citizens to say whatever they want, short of promoting violence or sedition. Other democracies are less absolute in their free-speech protections, but nonetheless agree on the underlying principle that there should be an open marketplace of ideas in which the government should play a minimal role.

The real problem centers around the platforms’ ability to either amplify or silence certain messages, and to do so at a scale that can alter major political outcomes. Any policy response should not aim at silencing speech deemed politically harmful. The notion that Donald Trump won the 2020 presidential vote in a landslide and that the Democrats stole the election through massive fraud is false and terribly damaging to U.S. democracy. But it is also sincerely believed by tens of millions of Americans, and it is neither normatively acceptable nor practically possible to prevent them from expressing opinions to this effect. For better or worse, people holding such views need to be persuaded, and not simply suppressed.

What policy needs to target instead is the dominant platforms’ power to either amplify or silence certain voices in the political sphere. Up to now we have been relying on people such as Twitter’s CEO Jack Dorsey or Facebook’s Mark Zuckerberg to “do the right thing” and curate harmful political content. This is a response that may work in the short run, when the nation is faced with an imminent threat of political violence. But it is not a long-term solution to the underlying problem, which is one of excessively concentrated power.

#### Interoperability enables middleware startups that ride on top of platforms but alter their content moderation decisions – competition is key because dominant platforms have no incentive to police information.

Fukuyama ’21 [Francis; Mosbacher Director @ Stanford’s Center on Democracy, Development and the Rule of Law; “Making the Internet Safe for Democracy,” *Journal of Democracy*, 32(2), p. 37-44]

Remedies

How can we reduce the underlying power of today’s internet platforms? I believe that a potential solution to this problem lies in using both technology and regulation to outsource content curation from the dominant platforms to a competitive layer of “middleware companies.” I advance this proposal not because I am certain that it will work, but because the alternative approaches that have been suggested are likely to be less effective.

The first and most obvious of these approaches is to use antitrust law to break up Facebook and Google, much as the telephone giant AT&T was broken up in the 1970s. After a prolonged period of lax enforcement of antitrust laws, there is a growing consensus that they need to be applied to the big tech companies, and suits have been brought against these platforms by the European Commission, the Justice Department, the Federal Trade Commission, and a coalition of state attorneys-general.

Breaking up these companies would indeed reduce their power over politics. But under current U.S. and EU laws, reaching a decision in the courts could take over a decade, as past antitrust cases against IBM and Microsoft did. More important, network externalities suggest that a baby Facebook emerging out of such a breakup could grow much faster than AT&T did when it was divided, and quickly reach the size of its parent. Antitrust law in any case is designed primarily to remedy the familiar harms stemming from concentrations of economic power, not the novel political risks produced by social media. What might realistically come out of current antitrust initiatives will be constraints on the platforms’ acquisition of startups, or on their recourse to vertical-tying agreements (policies that compel users of a product offered by one of the tech giants to procure a related service from that same company). Yet outcomes of this kind will not address the political problems posed by platform scale.

A second obvious remedy is government regulation, something that both the EU and individual EU member states have already sought to put in place. Germany’s NetzDG law, for example, imposes hefty fines on companies which fail to remove content that is illegal in that country within a day once it has been reported. There are precedents in the United States for government regulation of the content distributed by major media platforms. Back in the 1960s, when the television networks enjoyed an oligopolistic control over political discussion somewhat similar to the growing dominance of today’s social-media platforms, the Federal Communications Commission (FCC) used its licensing power to enforce the Fairness Doctrine, which required large media outlets to present competing points of view. The Fairness Doctrine’s constitutionality was upheld in the 1969 Supreme Court decision in Red Lion Broadcasting Co. v. FCC, but was relentlessly attacked thereafter by Republicans who felt that the FCC was biased against conservatives. The Fairness Doctrine was rescinded in 1987 through an administrative decision by the FCC, and attempts by Democrats to restore it were unsuccessful. While some European democracies retain enough of a social consensus to muster a mandate for content regulation, the United States today is far too polarized to be able to authorize the FCC or any other government body to determine what is “fair and balanced” and enforce such strictures against the internet platforms. Regulation therefore seems to be a dead end in the United States at the present moment.

A third approach to reducing platform power that has been put forward is data portability. The idea is that individual users own their data and should be able to move it to alternate platforms, just as they transfer their mobile-phone numbers from one carrier to another. While this approach sounds like an appealing way to increase competition among platforms, it runs into immediate difficulties involving both property rights and technical feasibility. For the platforms’ purposes, the most important data that they hold is not personal data voluntarily surrendered to them by users, but the mountains of metadata created by the users’ interaction with their platforms. It is legally not clear who owns metadata, and the platforms will fight to keep control over such data since this is the bedrock of their business models. Moreover, these data are hugely heterogeneous and platform-specific. Data portability is therefore not a way of addressing the political threat that platform power poses.

Finally, some have suggested that platform power might be kept in check by applying privacy legislation to keep the platforms from using data collected in one sphere, such as book retailing, in another, such as selling groceries or diapers (something that Amazon has done), without getting explicit consent from users. Such restrictions are already built into Europe’s General Data Protection Regulation (GDPR). Experience with that law, however, indicates that such rules are very hard to enforce; in any event, the United States does not have a privacy regime comparable to GDPR in place at the national level. Moreover, when it comes to the power of existing tech giants, the cat is already out of the bag, so to speak: Google and Facebook have already amassed huge databases on their users which privacy restrictions limiting future data collection would not touch.

Middleware

Given the inadequacy of these various approaches, it is worth taking a closer look at the alternative remedy that the Stanford Working Group on Platform Scale has labeled “middleware.” Middleware is software that rides on top of a platform and affects the way in which users interact with the data that the platform carries. A properly constructed middleware intermediary could, for example, filter platform content not just to label but to eliminate items deemed false or misleading, or could certify the accuracy of particular data sources. At one extreme, middleware could take over the entire user interface of a Facebook or Google, relegating those platforms to the status of “dumb pipes” that simply serve up raw data, much like the telephone companies. At the other extreme, middleware could operate with a light touch, labeling but otherwise not affecting the content-curation decisions being made by the platforms. This would resemble steps that Twitter has already taken to label certain types of content deemed misleading, including election news in the runup to the November 2020 U.S. elections, but would allow users to choose from a broader menu of labeling options. There currently exist third-party services, such as NewsGuard, that plug into web browsers to offer users ratings of the credibility of news sources that they encounter. Middleware could perform a similar function while plugging directly into the social media platforms. It could also transform the relationship between users and platforms in more fundamental ways.

Middleware could reduce the platforms’ power by taking away their ability to curate content, and outsourcing this function to a wide variety of competitive firms which in effect would provide filters that would be tailorable by individual users. When you signed up to Facebook or Google, you would be given a choice of middleware providers that would allow you to control your feed or searches, just like you now have a choice of browsers. In place of a nontransparent algorithm built into the platform, you could decide to use a filter provided by a nonprofit coalition of universities that would vouch for the reliability of data sources, or one that limited the display of products to those manufactured in the United States, or those that are environmentally friendly.

One of the likely objections to the middleware concept is that it will simply reinforce the “filter bubbles” that already exist on the platforms. Alt-right ideologues and conspiracy theorists could construct filters of their own that would keep out contrary views, leading to a further fragmentation of the political space. But as noted above, the objective of policy should not be to suppress harmful content. The latter, if it falls short of calling for violence, is constitutionally protected. In any event, it will be technologically very hard to eliminate such content. After the January 6 attack on the U.S. Capitol, extremists began to move to the new platform Parler (which prided itself on a minimalist approach to moderation), and then, when Parler was temporarily offline after being dropped by Amazon’s web-hosting service, to encrypted messaging services such as Telegram or Signal.

Much as we may regret this fact, hate speech and conspiracy theories are embedded in the broader society, and middleware will do little to stamp them out. But that is not a proper policy objective in a society that values free speech. What middleware might do instead is dramatically dilute the power of the platforms to amplify fringe views and take them mainstream. We might think of this in terms of an infectious-disease analogy: Instead of encouraging infected people to mingle in the broader society, we should seek to isolate them in spaces they share with the already infected.

Middleware will not spontaneously arise out of market forces. While there is demand for such services, there is no clear business model that will make them viable today. The platform owners may be happy to be relieved of responsibility for making controversial political decisions in their content moderation; in fact, Twitter’s Jack Dorsey himself has recently suggested “giving more people choice around what relevance algorithms they�re using,” adding: “You can imagine a more market-driven and marketplace approach to algorithms.”1 On the other hand, big tech will not like the loss of control that middleware intermediation creates. This means that the creation of a vibrant and competitive middleware sector will depend on government regulation, both to establish rules for the application programming interfaces (APIs) by which such companies would plug into the platforms, and to set revenue-sharing mandates that will ensure a viable business model for middleware purveyors. These are all issues that need to be fleshed out in greater detail as we think through the consequences of the political crisis we have faced.

Prospects

More and more people are coming to the realization that modern technology has created something of a monster, a communications system which bypasses the once-authoritative institutions that used to structure democratic discourse and provide citizens with a common base of factual knowledge over which they could deliberate. The private companies that are responsible for this outcome are now among the largest in the world. They possess not only enormous wealth which they can use to protect their interests, but also something of a chokehold over the communications channels that facilitate democratic politics. They benefit from economies of scale that are inherent in networked systems, and there is no easy way to prevent them from getting even larger. The covid-19 pandemic that struck the world in 2020 has vastly increased their power and importance.

Up to now, the large platforms have not seen it as in their interests to deliberately manipulate political outcomes or electoral results. Their commercial interests have, however, motivated them to privilege certain forms of viral content that more often than not are fake, conspiracy-laden, and harmful to democratic practice. What we should be worried about in terms of democratic health is the underlying power that these platforms possess. Public policy needs to be deployed to reduce that power, which otherwise might well one day come under the control of owners who do want to deliberately manipulate elections.

#### International enforcement responds to global reach of platforms in fragile democracies.

Fukuyama ’21 [Francis; Mosbacher Director @ Stanford’s Center on Democracy, Development and the Rule of Law; “Making the Internet Safe for Democracy,” *Journal of Democracy*, 32(2), p. 37-44]

Many people have come to see the internet as one of the chief threats to contemporary democracy. The internet, and large platforms such as Google, Facebook, and Twitter in particular, have been blamed for the rise of Donald Trump and the populism he represents, the proliferation of conspiracy theories and fake news, and the intense political polarization afflicting the United States as well as many other democracies. Across the world, politicians with authoritarian leanings, such as Rodrigo Duterte in the Philippines and Narendra Modi in India, have made effective use of Facebook and Twitter to reach their followers and attack opponents.

There is, nonetheless, a great deal of confusion as to where the real threat to democracy lies. This confusion begins with a question of causality: Do the platforms simply reflect existing political and social conflicts, or are they actually the cause of such conflicts? The answer to that question will in turn be key to finding the appropriate remedies.

This issue came to a head in the aftermath of the 6 January 2021 mob assault on the U.S. Congress that was instigated by the outgoing President Trump. In the wake of that violence, Twitter shut down Trump’s account, cutting him off from the primary channel that he had used to communicate with his followers. While many people applauded this decision and even saw it as overdue, others worried about the sheer power that Twitter had amassed. President Trump was indeed effectively muzzled in the days following the ban. Conservatives immediately castigated the move—and the parallel actions by Facebook, Google, and Amazon that soon followed—for what they labeled “censorship.” And while one may approve of Twitter’s decision as a short-run response to the danger of violent incitement, conservative critics of this move raise legitimate points about the dangers of platform power.

Legally speaking, the censorship charge falls flat. In U.S. law, the First Amendment’s prohibition of censorship applies only to government actions; the Amendment actually protects the right of private parties such as Twitter and Facebook to publish whatever content they want. Beyond these protections, online platforms have been shielded from certain forms of liability by Section 230 of the 1996 Communications Decency Act. The problem we face today, however, is one of scale: These platforms are so large that they have come to constitute a “public square” within which citizens contest issues and ideas. There are plenty of private corporations that curate the information they publish; these are media companies, with names such as the New York Times or the Wall Street Journal. But none of these legacy media companies is as dominant or reaches as many people as Twitter, Facebook, and Google. The scale of these internet platforms is great enough that decisions made by their owners could impact the outcome of democratic elections in a way that legacy media companies� decisions could not.

The other big problem with the large internet platforms is one of transparency. While Twitter publicly announced its ban of President Trump, it, Facebook, and Google make literally thousands of content-curation decisions each day. The great mass of takedowns are relatively uncontroversial, as with those targeting terrorist incitement, child pornography, or overt criminal conspiracies. But some decisions to flag or remove posts have been either more contentious or simply erroneous, particularly since the platforms began to rely increasingly on artificial-intelligence (AI) systems to moderate content during the covid-19 pandemic. An even more central question concerns not what content social-media platforms remove, but rather what they display. From among the vast number of posts made on Twitter or Facebook, the content we actually see in our feeds is selected by complex AI algorithms that are designed primarily not to protect democratic values, but to maximize corporate revenues. It is thus unsurprising that these platforms have been blamed for propagating conspiracy theories, slander, and other toxic forms of viral content: This is what sells. Users do not know why they are seeing what they see on their feeds, or what they are not seeing because of the decisions of an invisible AI program.

Harms

We thus need to be precise about the nature of the threat that the large platforms pose to modern liberal democracy. It does not lie in the mere fact that they carry “fake news” or conspiracy theories or other kinds of harmful political content. The U.S. First Amendment protects the right of citizens to say whatever they want, short of promoting violence or sedition. Other democracies are less absolute in their free-speech protections, but nonetheless agree on the underlying principle that there should be an open marketplace of ideas in which the government should play a minimal role.

The real problem centers around the platforms’ ability to either amplify or silence certain messages, and to do so at a scale that can alter major political outcomes. Any policy response should not aim at silencing speech deemed politically harmful. The notion that Donald Trump won the 2020 presidential vote in a landslide and that the Democrats stole the election through massive fraud is false and terribly damaging to U.S. democracy. But it is also sincerely believed by tens of millions of Americans, and it is neither normatively acceptable nor practically possible to prevent them from expressing opinions to this effect. For better or worse, people holding such views need to be persuaded, and not simply suppressed.

What policy needs to target instead is the dominant platforms’ power to either amplify or silence certain voices in the political sphere. Up to now we have been relying on people such as Twitter’s CEO Jack Dorsey or Facebook’s Mark Zuckerberg to “do the right thing” and curate harmful political content. This is a response that may work in the short run, when the nation is faced with an imminent threat of political violence. But it is not a long-term solution to the underlying problem, which is one of excessively concentrated power.

No democracy can rely on the good intentions of particular powerholders. Numerous strands of modern democratic theory uphold the idea that political institutions need to check and limit arbitrary power regardless of who wields it. This principle is implicit in John Rawls’s concept of the “veil of ignorance,” according to which fair rules in a liberal society must be drawn up without regard to knowledge of the person or persons to whom they apply. The 1780 Constitution of the State of Massachusetts, drafted by John Adams, Samuel Adams, and James Bowdoin, stated that “the executive shall never exercise the legislative [or] judicial powers . . . to the end it may be a government of laws and not of men.” James Madison’s famous Federalist 51 lays the ground for a system of divided powers by arguing that “in framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.” The only practical solution to this problem was to comprehend “in the society so many separate descriptions of citizens as will render an unjust combination of a majority of the whole very improbable, if not impracticable.” In other words, power could be controlled only by dividing it, through a system of checks and balances.

The authors of these strictures were taking aim at state power, but their concerns apply doubly to concentrations of private power. Private power faces no checks comparable to popular elections; it can be controlled only by the government (through regulation) or by competition among power holders. Due to a traditional suspicion of state power, market competition has generally been the preferred means of controlling and limiting private power in the United States. Fear of monopoly power’s economic and political consequences, among other concerns, inspired passage of the legislation making up the backbone of U.S. antitrust law—the Sherman (1890), Clayton (1914), and Federal Trade Commission (1914) Acts.

Remedies

How can we reduce the underlying power of today’s internet platforms? I believe that a potential solution to this problem lies in using both technology and regulation to outsource content curation from the dominant platforms to a competitive layer of “middleware companies.” I advance this proposal not because I am certain that it will work, but because the alternative approaches that have been suggested are likely to be less effective.

The first and most obvious of these approaches is to use antitrust law to break up Facebook and Google, much as the telephone giant AT&T was broken up in the 1970s. After a prolonged period of lax enforcement of antitrust laws, there is a growing consensus that they need to be applied to the big tech companies, and suits have been brought against these platforms by the European Commission, the Justice Department, the Federal Trade Commission, and a coalition of state attorneys-general.

Breaking up these companies would indeed reduce their power over politics. But under current U.S. and EU laws, reaching a decision in the courts could take over a decade, as past antitrust cases against IBM and Microsoft did. More important, network externalities suggest that a baby Facebook emerging out of such a breakup could grow much faster than AT&T did when it was divided, and quickly reach the size of its parent. Antitrust law in any case is designed primarily to remedy the familiar harms stemming from concentrations of economic power, not the novel political risks produced by social media. What might realistically come out of current antitrust initiatives will be constraints on the platforms’ acquisition of startups, or on their recourse to vertical-tying agreements (policies that compel users of a product offered by one of the tech giants to procure a related service from that same company). Yet outcomes of this kind will not address the political problems posed by platform scale.

A second obvious remedy is government regulation, something that both the EU and individual EU member states have already sought to put in place. Germany’s NetzDG law, for example, imposes hefty fines on companies which fail to remove content that is illegal in that country within a day once it has been reported. There are precedents in the United States for government regulation of the content distributed by major media platforms. Back in the 1960s, when the television networks enjoyed an oligopolistic control over political discussion somewhat similar to the growing dominance of today’s social-media platforms, the Federal Communications Commission (FCC) used its licensing power to enforce the Fairness Doctrine, which required large media outlets to present competing points of view. The Fairness Doctrine’s constitutionality was upheld in the 1969 Supreme Court decision in Red Lion Broadcasting Co. v. FCC, but was relentlessly attacked thereafter by Republicans who felt that the FCC was biased against conservatives. The Fairness Doctrine was rescinded in 1987 through an administrative decision by the FCC, and attempts by Democrats to restore it were unsuccessful. While some European democracies retain enough of a social consensus to muster a mandate for content regulation, the United States today is far too polarized to be able to authorize the FCC or any other government body to determine what is “fair and balanced” and enforce such strictures against the internet platforms. Regulation therefore seems to be a dead end in the United States at the present moment.

A third approach to reducing platform power that has been put forward is data portability. The idea is that individual users own their data and should be able to move it to alternate platforms, just as they transfer their mobile-phone numbers from one carrier to another. While this approach sounds like an appealing way to increase competition among platforms, it runs into immediate difficulties involving both property rights and technical feasibility. For the platforms’ purposes, the most important data that they hold is not personal data voluntarily surrendered to them by users, but the mountains of metadata created by the users’ interaction with their platforms. It is legally not clear who owns metadata, and the platforms will fight to keep control over such data since this is the bedrock of their business models. Moreover, these data are hugely heterogeneous and platform-specific. Data portability is therefore not a way of addressing the political threat that platform power poses.

Finally, some have suggested that platform power might be kept in check by applying privacy legislation to keep the platforms from using data collected in one sphere, such as book retailing, in another, such as selling groceries or diapers (something that Amazon has done), without getting explicit consent from users. Such restrictions are already built into Europe’s General Data Protection Regulation (GDPR). Experience with that law, however, indicates that such rules are very hard to enforce; in any event, the United States does not have a privacy regime comparable to GDPR in place at the national level. Moreover, when it comes to the power of existing tech giants, the cat is already out of the bag, so to speak: Google and Facebook have already amassed huge databases on their users which privacy restrictions limiting future data collection would not touch.

Middleware

Given the inadequacy of these various approaches, it is worth taking a closer look at the alternative remedy that the Stanford Working Group on Platform Scale has labeled “middleware.” Middleware is software that rides on top of a platform and affects the way in which users interact with the data that the platform carries. A properly constructed middleware intermediary could, for example, filter platform content not just to label but to eliminate items deemed false or misleading, or could certify the accuracy of particular data sources. At one extreme, middleware could take over the entire user interface of a Facebook or Google, relegating those platforms to the status of “dumb pipes” that simply serve up raw data, much like the telephone companies. At the other extreme, middleware could operate with a light touch, labeling but otherwise not affecting the content-curation decisions being made by the platforms. This would resemble steps that Twitter has already taken to label certain types of content deemed misleading, including election news in the runup to the November 2020 U.S. elections, but would allow users to choose from a broader menu of labeling options. There currently exist third-party services, such as NewsGuard, that plug into web browsers to offer users ratings of the credibility of news sources that they encounter. Middleware could perform a similar function while plugging directly into the social media platforms. It could also transform the relationship between users and platforms in more fundamental ways.

Middleware could reduce the platforms’ power by taking away their ability to curate content, and outsourcing this function to a wide variety of competitive firms which in effect would provide filters that would be tailorable by individual users. When you signed up to Facebook or Google, you would be given a choice of middleware providers that would allow you to control your feed or searches, just like you now have a choice of browsers. In place of a nontransparent algorithm built into the platform, you could decide to use a filter provided by a nonprofit coalition of universities that would vouch for the reliability of data sources, or one that limited the display of products to those manufactured in the United States, or those that are environmentally friendly.

One of the likely objections to the middleware concept is that it will simply reinforce the “filter bubbles” that already exist on the platforms. Alt-right ideologues and conspiracy theorists could construct filters of their own that would keep out contrary views, leading to a further fragmentation of the political space. But as noted above, the objective of policy should not be to suppress harmful content. The latter, if it falls short of calling for violence, is constitutionally protected. In any event, it will be technologically very hard to eliminate such content. After the January 6 attack on the U.S. Capitol, extremists began to move to the new platform Parler (which prided itself on a minimalist approach to moderation), and then, when Parler was temporarily offline after being dropped by Amazon’s web-hosting service, to encrypted messaging services such as Telegram or Signal.

Much as we may regret this fact, hate speech and conspiracy theories are embedded in the broader society, and middleware will do little to stamp them out. But that is not a proper policy objective in a society that values free speech. What middleware might do instead is dramatically dilute the power of the platforms to amplify fringe views and take them mainstream. We might think of this in terms of an infectious-disease analogy: Instead of encouraging infected people to mingle in the broader society, we should seek to isolate them in spaces they share with the already infected.

Middleware will not spontaneously arise out of market forces. While there is demand for such services, there is no clear business model that will make them viable today. The platform owners may be happy to be relieved of responsibility for making controversial political decisions in their content moderation; in fact, Twitter’s Jack Dorsey himself has recently suggested “giving more people choice around what relevance algorithms they�re using,” adding: “You can imagine a more market-driven and marketplace approach to algorithms.”1 On the other hand, big tech will not like the loss of control that middleware intermediation creates. This means that the creation of a vibrant and competitive middleware sector will depend on government regulation, both to establish rules for the application programming interfaces (APIs) by which such companies would plug into the platforms, and to set revenue-sharing mandates that will ensure a viable business model for middleware purveyors. These are all issues that need to be fleshed out in greater detail as we think through the consequences of the political crisis we have faced.

Prospects

More and more people are coming to the realization that modern technology has created something of a monster, a communications system which bypasses the once-authoritative institutions that used to structure democratic discourse and provide citizens with a common base of factual knowledge over which they could deliberate. The private companies that are responsible for this outcome are now among the largest in the world. They possess not only enormous wealth which they can use to protect their interests, but also something of a chokehold over the communications channels that facilitate democratic politics. They benefit from economies of scale that are inherent in networked systems, and there is no easy way to prevent them from getting even larger. The covid-19 pandemic that struck the world in 2020 has vastly increased their power and importance.

Up to now, the large platforms have not seen it as in their interests to deliberately manipulate political outcomes or electoral results. Their commercial interests have, however, motivated them to privilege certain forms of viral content that more often than not are fake, conspiracy-laden, and harmful to democratic practice. What we should be worried about in terms of democratic health is the underlying power that these platforms possess. Public policy needs to be deployed to reduce that power, which otherwise might well one day come under the control of owners who do want to deliberately manipulate elections.

The objective of public policy should not be to control speech. Modern democracies abjured such control when they committed themselves to protecting freedom of expression. What we want, rather, are public policies that prevent private actors from using their power to artificially amplify or suppress certain types of speech, and that maintain a level playing field on which ideas can compete.

While much of the discussion here has focused on the United States and the current crisis in U.S. democracy, excessive platform power has worldwide repercussions. Facebook and Twitter are even more politically important in smaller countries around the globe, where they have become the major channel of public and private communication. In the wake of Twitter’s de-platforming of Donald Trump, critics immediately asked why similar decisions were not being made to curtail the antidemocratic behavior of other politicians around the world, from elected populists to rulers in autocracies, who have used incendiary rhetoric online. In India, for example, Facebook has been singled out for its failure to take down posts decried for fomenting violence against Muslims.

It is clear that these giant U.S. companies do not have anywhere near the capacity to make nuanced political judgements about the acceptability of speech in the roughly 150 countries in which they operate. It is very hard to see what would give them the incentive to acquire such capacity in the future. More important, they do not have the legitimacy to control speech in their home country, the United States, much less in other countries around the world.

This is why the diminution of platform power is critical for the survival of democracy around the world. While Europeans have made efforts to curb platform power, Americans up to now have been complacent about the issue. Now that there is a general consensus that the large platforms pose a danger to U.S. democracy, it is vital to understand precisely where that threat lies, and what remedies are both politically and technologically realistic.

#### Interoperability-enabled open data remedies algorithmic discrimination by providing real-time access to algorithms – sector-specific regulations and transparency fail.

Marsden ’19 [Chris; 9/19/19; Professor of Internet Law @ University of Sussex, PhD @ Essex; and Rob Nicholls; Associate Professor in Regulation and Governance @ UNSW Business School, PhD @ UNSW; “Interoperability: A solution to regulating AI and social media platforms”; <https://www.scl.org/articles/10662-interoperability-a-solution-to-regulating-ai-and-social-media-platforms>; \*Acronyms Expanded in Brackets]

Introduction

In the space of a few short years, Artificial Intelligence (AI) has leapt from the pages of science fiction to become a part of our everyday lives. Digital Era governance means decisions are taken about our lives by both government and private actors by their AI systems that can have potentially profound implications1. AI technologies “aim to reproduce or surpass abilities (in computational systems) that would require intelligence if humans were to perform them”2. AI is an advanced deployment of Machine Learning (ML). AI is the latest iteration of Machine Learning but is a very early stage of any defined Artificial General Intelligence that may achieve the hypothetical ‘singularity’ of self-consciousness as made infamous over fifty years ago by Stanley Kubrick’s cinematic interpretation of Arthur C. Clarke’s HAL90003. ML is in some respects a subset of human-computer interaction (HCI): that is algorithms applied to (big) data to aid human decisions.

AI is already deployed in ways that we may not even be aware of with incidents of abuse of that data reported daily. In this article, we argue there is a better, broad way to prevent abuse: interoperability. “Computer says no” cannot be the final answer to our quest for justice in such decisions. We argue that what is needed most urgently is a remedy to dominant consumer-facing platforms deploying AI in non-transparent systems. AI is being used in many systems, with little to no transparency, from facial recognition cameras in public spaces to removal of ‘fake news’ from social media platforms, yet consumers have no visibility of these technologies nor remedy if their rights are potentially infringed.In our view the answer is not just a temporary dose of transparency, which may not be feasible or even desirable4, but an interoperability remedy that lets regulators and potential rivals see inside the ‘black box’ to judge the AI for themselves5. There is a caveat: regulation may not be suitable, appropriate or feasible for many algorithms but for those that regulators have most concern about, in sectors that provide the most sensitive socioeconomic decisions, it is a remedy that can be explored. Sensitive public facing sectors may include: banking/credit, insurance, healthcare & medical research, social care, policing and security, education, transport (AI-guided airliners & automated vehicles), social media, telecommunications6. This is a non-exclusive list that may be altered by emerging public techno-socio-policy concerns.

How is AI governed in practice?

At present, AI is largely governed through self-regulation and the technology giants, including the GAFAM/FAANG platform operators7, appear set on persuading us that self-regulation remains the only effective route to legal accountability for machine learning systems. Such an attitude jeopardises the sustainable introduction of smart contracts, permitting algorithmic discrimination and compromising the implementation of privacy law8.

Recent public policy focus on digital decision-making has led to a wider debate about computer-aided adjudication. Legal focus has exposed discrimination that occurs in machine learning parsed into their interaction9. Discriminatory data is likely to lead to discriminatory results. Discriminatory algorithms - as well as those not designed to filter out discrimination - can make those results more discriminatory. Justice requires that lawyers study algorithmic outcomes in order to ascertain such discrimination, which may be highly inefficient as well as outrageous to natural justice and fundamental rights. Public administration has generic solutions. Administrative law requires natural justice, or at least, ‘reasonableness’. A right to explanation and / or remedy should apply, and anti-discrimination law also applies to corporate decisions. AI decision making has raised the question: is the decision maker AI or human?

The case of UK Visa applications demonstrates that AI is not a trustworthy contributor to what was already never a happy or exact science. The UK government minister (at the time of writing) claimed that use of AI in visa applications was acceptable as humans made the final decision: “Sifting is not decision making”10. The Council of Europe in principle disagrees: while to err is human, inducing AI complexity does not absolve the operator of responsibility for harms11.

Our focus in this article is on the private activities of private companies, particularly in networked industries that affect consumers at scale. We now have a variety of pro-consumer/citizen laws that extend rights and obligations far beyond classical freedom of contract, including: anti-discrimination and equality laws; financial regulation; consumer contract law; and telecommunications regulation. Specialist technology law is deployed in many fields that now make up the Information Society: biomedical/nanotechnology deployment; railways, roads, and telecoms; data protection12. Judges may solve problem in tort/contract, though this took 100 years in case of railways litigation, and it would require many technologically savvy judges, and a large number of leading cases in common law jurisdictions to achieve the same outcome. In contrast, the largest civil law system, European Union consumer law, is pressing ahead with legislation to combat AI injustice before the end of 2019, President-elect Von der Leyen stating: “In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence.”13 The new President also promised a new Digital Services Act to regulate large digital platforms. Our proposed solution will approach both issue areas coherently.

Transparency, replicability and general data protection are incomplete solutions to AI

Transparency is the first requirement of legal recourse (though some algorithms can be reverse engineered without transparency “under the hood” of the machine). It is not sufficient, however, for several reasons. Claims that the ability to study an algorithm and its operation provides a remedy for users who suffer as result of decisions falls short for one simple reason: both the training data and the algorithm itself will change constantly. For instance, it is impossible to forecast real time outcomes of Google searches; a vast Search Engine Optimization business attempts approximations without complete accuracy. The only remedy that can be achieved is replicability – taking an ‘old’ algorithm and its data at a previous point in time to demonstrate whether the algorithm and data became discriminatory. This is an incomplete a remedy as it in effect it uses a ‘slow motion replay’ while the game rushes onwards.

Wagner argues for the need for systematic redress by an external agency to instil confidence in AI decision making14. He uses AI deployment case studies to illustrate the point: self-driving cars, police searches using social media/Passenger Name Records, Facebook content moderation. All require minimal regulation for the public to get some trust in using these technologies (some of which are compulsory to use services or even enter countries). ‘Ethics washing’ is undertaken by technology companies and their professional advisors, where attempts are made to persuade policy makers that self-regulation is the only effective route to legal accountability for Machine Learning systems15. If this means the public distrusts AI and any system claiming to use AI, it may be jeopardizing the sustainable introduction of smart contracts, permitting algorithmic discrimination and compromising implementation of data protection law. Regulators are wise to these tricks. Ethics washing will fail16. Cursory research into history of communications regulation and Internet law demonstrates the falsity of this self-regulation proposition17.

The EU right to data portability (“RTDP”) under the GDPR18 might be seen as a partial solution to combat market concentration in EU. The current version of RTDP might be too limited, as portability only applies when the data subject herself provided the data, yet data is often a shared service with multiple owners and creators (consider a selfie photo of best friends, posted by both online in separate accounts with separate tags and hashtags). Further, it cannot be a general instrument of economic policy in digital markets, as data is “unlocked” solely if the data subject invokes RTDP under GDPR.19Edwards and Veale indicate RTDP is not enough and “regulation to promote true interoperability is vital”.20

Competition or communications/media regulation: What can and should be done?

Interoperability enables more free data flow, an essential but not sufficient input for data-driven innovation21. Open and interoperable standards can help to increase competition in digital markets. UK’s Open Banking Standards, designed to enhance competition in the banking sector by enabling fintech entrepreneurs entry to market, could be an appropriate example.22 However, interoperability will not always leads to more innovation and competition.23 Interoperability through uniform standards and interfaces, might limit companies development of their own innovative goods and services with specific components since they have to comply with the requirements of interoperability.24 Implementation of a maximum level of interoperability could also cause privacy harms. If technical and consumer control mechanisms are not well designed, interoperability might increase the risk of misuse of personal data due to multiple service providers access to user’s personal data. Therefore, open and interoperable standards should avoid overstandardization and serve pro-competitive goals.25

We therefore suggest three regulatory options for consumer-deployed AI regulation, though we only propose two should be made operational.

1. Ethical standards for all AI deployed in the ‘wild’ to the public. ISO standards should be implemented with basic privacy/human rights impact assessment.

2. Interoperability for public communications providers – Instant Messaging/Search/Social Media companies

3. API (Application Programming Interface) opened to dominant (Significant Market Power: SMP) operators. This is based on Microsoft remedies in longest, most expensive antitrust case in EC history: a case which started in 1993 and whose remedies, imposed in 2004, only expired at the end of 2014. The later Google antitrust case, started in 2009, is ongoing a decade later26.

Ethical standards for all AI deployed in ‘wild’ – to public

An industry standard could be a baseline for deploying sensitive technologies with cybersecurity and human rights impacts. ISO standards are being formed, and can be quite powerful influencers (see ISO27001 on cybersecurity for example). Typically technical engineering is a realm not considered suitable for normative standards.

However standards embedded in national laws can become a weak coregulatory signal. Basic privacy/human rights impact assessment has been proposed by UN Rapporteur Prof. David Kaye, and AI impact assessment suggested by Mantelero for the Council of Europe27. Standards Australia is chairing an ISO Working Party28.

More broadly, ethics standards for AI deployment have been suggested by many organisations. The European Union29 & OECD Guidelines may receive the widest acceptance30. Many other guidelines exist, such as: the US 2019 Executive Order on AI; UK Centre for Data Ethics and Innovation (CDEI) at Turing Institute31. Hosanagar advocates the creation of an independent Algorithmic Safety Board, modelled on the Federal Reserve Board32.

Why interoperate?

Connectivity and communication are an essential part of contemporary life whether it be individuals using social media or telecommunications, businesses interacting with one another or across government departments. Interoperability at its most basic level can be defined as the ‘ability of two or more systems or components to exchange information and to use the information that has been exchanged.’33

Interoperation is driven by economics: there is nothing less valuable than a network with one user. Interoperability results in increased value of several networks and promotes efficient investment in and use of infrastructure. It permits new entrants to compete with existing operators and promotes entry. Network effects of interoperability are based on a heuristic called Metcalfe's law. Metcalfe hypothesised that while the cost for the network to grow the number of connections is linear, its value would be proportional to the square of the number of users.34 The users and operators of each network gain according to more users of that network, and lose where users switch away to a more popular network.

There are social benefits of interoperability. It eliminates the consumer need to acquire access to every network or the tendency to a winner-takes-all outcome. This is inelegant from a device design perspective too: readers may remember when the US had different mobile design standards to the EU (CDMA rather than GSM). In Instant Messaging (IM), arguably the winner-takes-all is Facebook/WhatsApp/Instagram without interoperability – with all IMs inside the corporation becoming interoperable35.

Interoperability can be divided into technical or non-technical. Technical interoperability includes communications, electronic, application, and multi-database interoperability whilst non-technical interoperability includes organisational, operational, process, cultural and coalition interoperability.

Regulatory intervention can be applied to either but addressing the technological aspects of interoperability provides predictable regulation.

Interoperability option for public communications providers (PCPs)

Interoperability is not radical as a regulatory requirement. It is required for broadcasters to enable Electronic Programme Guides (EPGs), and telecoms companies for telephone numbering schemes. Co-regulatory standards are often used. A PCP interoperability proposal would not regulate public communications providers as utilities but as media providers, and this is not common carrier regulation nor equivalent to energy/postal providers. It is intended to regulate operators as printers, not publishers, with primary content liability remaining with individual user/authors. We note that attempts to impose ‘Duty of Care’ fiduciary in the UK and the US are highly inappropriate and anomalous to the entire history of Internet and analogue free speech and content regulation36.

Not all PCPs will wish to interoperate, not least because the large platform PCPs have been found to have insecure communications and compromised protocols, so smaller PCPs may refuse to interoperate even were the option available. A good example is data security and minimalization philosophy deployed by the founder of Signal (Cryptographer and Open Whisper Systems founder Moxie Marlinspike), a perspective that is shared in part by Telegram37. The PCP interoperability option can therefore only be adopted towards specific dominant operators, not all PCPs, without compromising cybersecurity innovation and the freedom of choice of individual users.

Opening Dominant operators’ APIs

Opening up the API enables brokers, comparator programmes, regulators to access algorithms in real time & controlled conditions, in order to observe the algorithm’s behaviour. Where an operator is found to be dominant, interoperability could be applied as a consumer remedy, not a competition one. EU Commissioner Vestager recently described her policy on interoperability and large platforms:

“Making sure that products made by one company will work properly with those made by others – can be vital to keep markets open for competition. Microsoft’s takeover of LinkedIn approval depended on agreement to keep Office working properly, not just with LinkedIn, but also with other professional social networks. The Commission will need to keep a close eye on strategies that undermine interoperability”38.

Recently, in a contested decision, the Australian ACCC found dominance by Facebook and Google39. Interoperability would only apply to platform aspects of their business, for example mobile app stores not Apple or Android phones. Three models have been proposed:

Model 1: Must-carry obligations, as used for regulating EPGs

Model 2: API disclosure requirements, as with Microsoft from EC rulings40.

Model 3: Interconnect requirements, which are applied to telecoms, especially operators with SMP41. Interoperability can be separated into three types, as identified in a recent study for DG Competition42:

Protocol interoperability: this provides the ability of services/products to interconnect technically. It is the ‘usual’ from of interoperability seen in competition policy, as between the Microsoft Windows operating system and the APIs of Internet browsers such as Firefox and Chrome.

Data interoperability: Recalling Mayer-Schonberger/Cukier and their remedy to ‘Big Data’ monopolists in their eponymous book, this would provide a slice of data to competitors43.

Full protocol interoperability, is what telecoms regulators often think of as full interconnection.

In principle, providing access to APIs is likely to be in the best interest of the service provider. That is, the provider gets the same network effect advantage set out above. However, if a service provider with SMP [significant market power] chooses to make an API private, this may represent a barrier to entry. If a service provider with SMP [significant market power] chooses not to make an API available, this may also represent a barrier to entry. If either of these conducts has the potential to substantially lessen competition, then an ex ante access regime to an API is a potential regulatory solution.

The requirements for such an access regime would be consistent with usual practice associated with either essential facilities or bottlenecks in networked industries. However, there will need to be slight differences in the regime, depending on whether access is to an otherwise private API or to an API that was required to be created as part of the ex ante regulation. The regulatory language required to impose the API obligation is similar to that required in telecommunications. The API provider is referred to as the access provider and the person seeking to use the API is referred to as an access seeker. As such, a preliminary stage of the ex ante regulation might well be to have a regime in which an access provider can make a standing API access offer by having either a public or private API to which access is offered on a non-discriminatory basis where the terms and conditions of access are set out in a Standard API Access Agreement (SAAA). The SAAA would form an offer, capable of acceptance by any member of a class of those qualified to become access seekers.

If there is no such SAAA, then the regulatory access obligation would be in the form set out below.

If the access provider has an API, then the access provider must, if requested to do so by an access seeker:

(a) supply access to the API to the access seeker;

(b) take all reasonable steps to ensure that the technical and operational quality of the API supplied to the access seeker is equivalent to that which the access provider provides to itself; and

(c) take all reasonable steps to ensure that the access seeker receives, in relation to the API, fault detection, handling and rectification of a technical and operational quality and timing that is equivalent to that which the access provider provides to itself.

If the access provider has created an API, then the access provider must, if requested to do so by an access seeker:

(a) supply access to the API to the access seeker; and

(b) take all reasonable steps to ensure that the access seeker receives, in relation to the API, equivalent technical, operational and data access outcomes to those that the access provider provides to itself.

The price of access to an API would usually be based on a building block model approach. In any case, it should return a normal profit to the access provider based on that access provider’s weighted cost of capital. There may be a requirement to provide a safety net set of non-price access terms and conditions in the absence of a SAAA.

Conclusion From Interoperability for Social Media Platforms Deploying AI to Broader Remedy?

We have explained in this article that AI is too dynamic an environment for transparency and replicability to provide a comprehensive solution for users who have suffered injustices. To really help the regulatory environment work in the public interest, we need to introduce interoperability for users and regulators to see ‘inside the black box’ of AI decision makers. Interoperability is not radical as a regulatory requirement and is required for broadcasters and telecoms companies to enable EPGs and telephone numbering schemes respectively. Co-regulatory standards are often used. This proposal would not regulate public communications providers as utilities but as media providers, and this is not common carrier regulation nor equivalent to energy/postal providers. It is intended not to regulate operators as publishers but as printers, with primary content liability remaining with individual user/authors. We are agnostic as to the location of an ‘interoperability regulator’ beyond noting that the deployment of AI is predicted to become so widespread throughout socio-economic arenas that a generic regulator may rapidly be more useful than a communications specific regulator. More research is needed as to whether ‘Ofcom’ should be supplanted or supplemented by ‘OffData’44.

Many research questions for digital competition remain. Interoperability is extensively used in sectors with which we are most familiar. Is this interoperability remedy more broadly applicable? Can self-driving vehicles or banking, insurance, medical algorithmic ‘AI’ be regulated using interoperability? It depends on a variety of socio-economic factors. Many sectors have regulators working on ‘regulatory sandpit’ solutions.

#### Unchecked algorithmic discrimination cause extinction.

Thomas ’21 [Mike; 7/21/21; Citing Stuart Russell, Professor of Computer Science and Smith-Zadeh Professor in Engineering @ UC Berkeley, Former Vice-Chair of Council on AI and Robotics @ World Economic Forum, PhD in Computer Science @ Stanford; Max Tegmark, PhD in Physics @ UC Berkeley, Professor of Physics @ MIT, Gold Medal Recipient @ Royal Swedish Academy of Engineering Sciences for AI research; “The Future of AI: How Artificial Intelligence Will Change the World”; <https://builtin.com/artificial-intelligence/artificial-intelligence-future>]

“There are several major breakthroughs that have to occur, and those could come very quickly,” Russell said during his Westminster talk. Referencing the rapid transformational effect of nuclear fission (atom splitting) by British physicist Ernest Rutherford in 1917, he added, “It’s very, very hard to predict when these conceptual breakthroughs are going to happen.”

But whenever they do, if they do, he emphasized the importance of preparation. That means starting or continuing discussions about the ethical use of A.G.I. and whether it should be regulated. That means working to eliminate data bias, which has a corrupting effect on algorithms and is currently a fat fly in the AI ointment. That means working to invent and augment security measures capable of keeping the technology in check. And it means having the humility to realize that just because we can doesn’t mean we should.

“Our situation with technology is complicated, but the big picture is rather simple,” Tegmark said during his TED Talk. “Most AGI researchers expect AGI within decades, and if we just bumble into this unprepared, it will probably be the biggest mistake in human history. It could enable brutal global dictatorship with unprecedented inequality, surveillance, suffering and maybe even human extinction. But if we steer carefully, we could end up in a fantastic future where everybody’s better off—the poor are richer, the rich are richer, everybody’s healthy and free to live out their dreams.”

#### Disinformation creates a breeding ground for Russian fake news campaigns – the plan inhibits Russian operatives.

Hendrickson ’17 [Clara; 12/7/17; Research Analyst @ Brookings; and William Galston; Ezra K. Zilkha Chair and Senior Fellow in Governance Studies @ Brookings; “Big technology firms challenge traditional assumptions about antitrust enforcement”; https://www.brookings.edu/blog/techtank/2017/12/06/big-technology-firms-challenge-traditional-assumptions-about-antitrust-enforcement/; AS]

THE NEW TECHNOLOGY TRUSTS

So while fear that big tech can wield excessive influence in our democracy may reflect broader misgivings outside the realm of antitrust law and enforcement, some political concerns about big tech appropriately fall under the purview of antitrust regulation. As Sally Hubbard, a Senior Editor at the Capitol Forum who covers monopolization issues, recently stated in an interview with Vox’s Sean Illing, “Companies like Facebook and Google have had an outsize effect on political discourse because of the ways their algorithms help to promote and spread fake news and propaganda. Even if it’s not their intent, their business model invariably contributes to this problem.” More competition between rival platforms would have introduced a greater number of algorithms for Russian operatives to navigate, and probably would have mitigated the impact of the fake news that successfully targeted voters during the 2016 U.S. election.

Similarly, because the services offered by the likes of Google and Facebook are free (or low cost in the case of Amazon), tech companies have escaped the predatory pricing concerns typically triggered by anticompetitive high prices. However, Financial Times columnist Rana Foroohar has argued that we incur non-monetary costs when we use these services, handing over our attention and personal data.

Of course these two examples do not immediately elicit a clear solution for antitrust enforcement reform one way or the other, but they do illustrate that the dynamics of the tech era will require an updated conception and application of current antitrust law. While what this looks like remains unclear, a consensus is emerging that the Chicago School consumer welfare framework, formulated by Robert Bork and Richard Posner among others, has failed to capture today’s market power. In a widely-read note published in the Yale Law Journal, Lina Khan, a fellow at the Open Markets Institute, shows that the focus on low prices as the exclusive goal of antitrust cannot account for Amazon’s dominance.

#### Russian propaganda campaigns cause miscalc – goes nuclear.

Trenin ’18 [Dmitri; 1/25/18; Director @ Carnegie Moscow Center; “Avoiding U.S.-Russia Military Escalation During the Hybrid War”; https://carnegiemoscow.org/2018/01/25/avoiding-u.s.-russia-military-escalation-during-hybrid-war-pub-75277; AS]

FEATURES OF THE HYBRID WAR

This Hybrid War’s most distinguishing feature is that it is being fought in a truly global, virtually borderless environment. International interaction is no longer restricted by walls or other state-imposed barriers. Traditional distinctions between strategy and tactics have been all but erased. The hybrid warriors include many more players than was the case during the Cold War—from national governments and transnational corporations to nongovernmental actors and even private individuals.

The war is being fought simultaneously in a number of spheres, on different levels, and in the never-ending, twenty-four-hour news cycle. This aspect of warfare is particularly true of the field of information, which is of prime importance in the Information Age that emerged with the end of the Cold War. From cyber conflicts and the use of artificial intelligence to the predominance of propaganda and fake news, the main battles of the Hybrid War are taking place outside of the purely physical realm and in the domain of new information technologies. Just as important to the Hybrid War is economics, which has been the key driver of globalization that paralleled the rise of these innovative information technologies. The prominence of the U.S. media and the United States’ immense financial power give it a huge advantage in both fields. As a result, the weapons of choice in the Hybrid War are those that use information and economic power to discredit and sanction one’s adversaries.3

Politically, the Hybrid War includes the outside stimulation of political changes in other countries through street activism and the promotion of specific values, parties, or popular movements. It has been characterized by interference in elections, political transitions, and other political processes, including various efforts to hack sensitive information, spread compromising or damaging materials and fake news, encourage character assassinations, and impose personal and other noneconomic sanctions (for example, restrictions on travel, seizure of assets, imprisonment, or deportation) on opponents. The existence of a common information space makes waging political warfare on foreign territory much easier and more attractive than ever before. Cross-border promotion of democracy and support for the color revolutions that dominated the 2000s (for example, the 2003 Rose Revolution in Georgia and the 2004 Orange Revolution in Ukraine) have now found counterparts in emerging solidarity among those who espouse more conservative and traditionalist values, such as political systems based on authoritarian models and strict national sovereignty.4

Military power is not out of the picture—though its use is different than in the Cold War. The static standoff of million-strong armies in Europe and the long shadow of the nuclear arms race have drawn down or faded. Nuclear deterrence between Russia and the West remains in place but at lower and more stable levels than during the Cold War. Today’s risks of miscalculation derive from potential incidents involving conventional forces. A token military standoff has reemerged along Russia’s border with NATO countries, but, to date, this standoff bears no resemblance in either scale or scope to the forces that faced each other during the Cold War. The main focus is on developing new military technologies and novel means and ways of prosecuting warfare—from outer space to cyberspace—that blur or eliminate the distinction between wartime and peacetime. Like its predecessor, the Hybrid War is a war in the time of peace. Even more than in the past, however, the onus is on national leaderships to minimize the number of casualties, ideally to zero.

Russian military strategists had developed the concept of hybrid warfare even before the actual conflict broke out in earnest between the United States and Russia in early 2014. Analyzing the experience of the post-Soviet color revolutions and the 2011 Arab Spring, Chief of the General Staff Valery Gerasimov wrote in February 2013 that the “consequences of new conflicts are comparable to those of a real war”; in many cases, nonmilitary methods “are substantially more effective than the power of arms,” and greater emphasis is placed on “political, economic, information, humanitarian, and other nonmilitary means” and “covert military measures,” including “information warfare and actions by special forces.” In this environment, “overt use of military force, often in the form of peacekeeping or crisis management, takes place only at a certain stage, mainly to achieve final success in a conflict.” With regard to the U.S.-Russia confrontation, another key feature has surfaced: asymmetry between the sides’ capabilities.

POWER ASYMMETRIES AND ASYMMETRIC ACTIONS

Although Gerasimov was referring to a hybrid war when discussing new means and methods of warfare, this analysis uses the newly fashionable term to describe the current U.S.-Russia confrontation. Unlike its Cold War predecessor, this conflict is asymmetrical. At least since the 1970s, the Soviet Union was the United States’ equal in terms of both nuclear and conventional military power. Even beyond its own vast land mass and immediate sphere of influence in Eastern Europe, it wielded considerable ideological power in many Western countries and in the Third World and presided over a system of alliances in Africa, Asia, Europe, Latin America, and the Middle East. The Russian Federation, by contrast, has few formal allies, no satellite states, and a handful of protectorates, if one includes the self-proclaimed states of Abkhazia, Donbass, South Ossetia, and Transnistria. It has no ideology to compare with the comprehensive dogma of Marxism-Leninism, and although it is still a nuclear superpower, it lags far behind the United States in non-nuclear military capabilities. Economically, Russia—with its estimated 1.5 percent of the global gross domestic product—is a dwarf.

Neither the balance nor the correlation of forces, however, will determine the outcome of this confrontation. Despite the glaring asymmetries in the national power of the two sides of the conflict, the course of events is not predetermined. As a nonlinear, highly asymmetrical conflict, the outcome likely will result from domestic developments in Russia or the United States or both. Both countries are facing serious problems that could prove decisive in the final calculations of the Hybrid War.

The United States is going through a triple crisis of its political system, exemplified but not caused by the arrival of President Donald Trump and the virulent domestic opposition to him and his policies. A crisis of social values lies beneath this political crisis and points to a widening gap between the more liberal and the largely conservative parts of the country. At the same time, the United States faces a crisis within its own foreign policy as it struggles to reconcile the conflict between the more inward-looking U.S. national interest and the international liberal order of the U.S.-led global system.

Russia, though outwardly stable, is approaching its own major crisis as the political regime created by Putin faces an uncertain future after the eventual departure of its figurehead. Putin’s Kremlin is already working on a political transition that would rejuvenate the elite and improve its competence and performance, but, at the same time, Russian society is also changing and Putin’s heirs cannot take its support for granted. Gross inequality, sluggish economic growth, low vertical mobility, and high-level corruption will present a range of serious challenges to the future Russian leadership.

The eventual outcome of the Hybrid War could be reminiscent of the downfall of the Soviet Union, which was far less the result of the U.S.-Soviet Cold War than of a misguided effort to reform the Soviet Union itself. Russia might break down and break up again, or it might decide on a foreign policy more geared toward its economic needs than to a certain concept of world order. As for the United States, it might decide to limit its global commitments and redesign its international role as the world’s preeminent but no longer dominant state. Yet, in doing so, it will need to accept that its change in status will come with a certain price and that it will not be able to take advantage of the benefits of the position it once enjoyed.

Asymmetries in power lead to asymmetric actions, which as Gerasimov suggested are intended to “neutralize the enemy’s superiority in warfare” or “identify and exploit the enemy’s vulnerabilities.”5 By an order of magnitude—or more—Russia is outgunned, outmanned, and outspent by the combined forces of the United States and its allies. To stay in the fight, it must rely on its few comparative advantages and seek to use them to maximum effect. These advantages include the geographical proximity of some of the main theaters of operation, such as Crimea and eastern Ukraine, where Russia has escalation dominance; the Russian political system, which allows for secretive, swift, and decisive action; and Moscow’s willingness to take much higher risks in view of the disproportionally higher stakes involved for the Russian leadership and a national culture that historically has tolerated higher losses in defense or protection of the Motherland. Through swift decisions and actions, made without prior warning, Russia is capable of surprising its adversaries and keeping them off-balance. This situation promises an uncertain, hard-to-predict, and risky environment, where miscalculation can lead to incidents or collisions that, in turn, lead to escalation. Granted, these incidents would be of a different kind than the tank standoff at Berlin’s Checkpoint Charlie in late October 1961 or the Cuban Missile Crisis barely a year later. Escalation resulting from miscalculation would not be automatic, but the wider damage it could cause needs to be taken seriously.

#### Platform misinformation fuels Hindu nationalism.

Pahwa ’21 [Nitish; 10/26/21; Editor @ Slate; "The Facebook Crisis in India Might Be the Worst Facebook Crisis of All”; https://slate.com/technology/2021/10/facebook-papers-india-modi-misinformation-rss-bjp.html]

Thanks to whistleblower Frances Haugen’s testimony and the news articles based on documents she leaked, the public has gained an alarming new perspective on how Facebook ignored, downplayed, or failed to adequately address harassment, mis- and disinformation, and incitements to violence on its platform in several major countries. The documents, which CNN claims could be “the biggest crisis” in Facebook’s history, have revealed just how the network became an incubator of hate and terrorism from the U.S. to Ethiopia. Yet the most shocking revelations concern the nation that serves as the app’s biggest user base: India, the world’s largest backsliding democracy.

Reports of social media–fueled horrors within India—attacks on Muslims, lower-caste peoples, women, the poor, and refugees—have been troublingly commonplace for a half-decade now. Yet what the Facebook Papers confirm is not just that the network failed to curb Hindu nationalist hate speech and inadequately directed resources to monitor a nation with 340 million users; it also actively granted impunity to the worst offenders. And according to Haugen, this was one of her foremost concerns when she began to reach out to reporters with the internal information she held.

Let’s start with the first point. According to the Verge, at the end of 2019 Facebook placed India within “tier zero,” meaning it was one of the countries of utmost priority for the network’s harm-reduction efforts. (The timing here is noteworthy, as India had then erupted in mass protests against an Islamophobic law, which continued until an ugly anti-Muslim pogrom months later effectively deflated the rallies.) Yet Facebook was far more focused on another “tier zero” country: the U.S. Per the New York Times, “Eighty-seven percent of the company’s global budget for time spent on classifying misinformation is earmarked for the United States, while only 13 percent is set aside for the rest of the world.” In other words, the bulk of attention was directed toward a country that doesn’t even have as many people as India has Facebook users. Furthermore, the company’s “misinformation classifiers”—automated systems trained on machine learning to detect and take down posts with harmful falsehoods—were not developed enough to recognize and take action on millions of multilanguage disinformation posts that proliferated across Indian feeds.

The result was that Facebook simply missed huge amounts of misinformation, even as it kept touting the ability of its internal tech to detect and take down false news. The company invested in uncovering hate speech written in Hindi and Bengali, two of India’s major languages—even though the country as a whole has 22 constitutionally recognized languages and hundreds more dialects. These limitations also meant that Facebook was ill-equipped to stop the virtual human trafficking of Indian domestic workers. Not to mention, there were spillover effects from inaction in other countries: Myanmar’s ethnic cleansing of Rohingya Muslims was amplified by the network, and thousands of refugees streamed to India, where they’ve faced further persecution.

Facebook also clearly took sides when it came to Indian violence.

When Narendra Modi was elected India’s prime minister in 2014, there were plenty of reasons for any democracy-favoring thought leader to be concerned: his oversight of fatal Hindu-Muslim riots when he was chief minister of the state of Gujarat, his historic ties to the Hindu nationalist Rashtriya Swayamsavek Sangh organization, and his political party’s use of Islamophobia as a campaign tactic—a successful one for the far-right Bharatiya Janata Party, many of whose members stemmed from the RSS. Yet none of this dissuaded Facebook CEO Mark Zuckerberg from literally embracing Modi during his first years in power. After all, Modi’s campaign made ample use of Facebook and other social networks, and the new PM was eager to work with Silicon Valley firms to modernize India’s internet experience.

But as I noted just earlier this year, reports of BJP-linked cells using Facebook and WhatsApp to spread toxic rhetoric and lies surfaced as early as 2016; more such troll operations proliferated in the subsequent years, both within and without election contexts, and led directly to lynchings of religious minorities and riots stirred up by aggrieved Hindus. As revealed by the leaked documents, Facebook did carry out thorough probes surveying the rot of Indian social media content; an employee who spearheaded the research noted that “I’ve seen more images of dead people in the past three weeks than I’ve seen in my entire life total. … [The feed] is a near constant barrage of polarizing nationalist content, misinformation, and violence and gore.” According to the Wall Street Journal, investigators zoned in on two BJP-linked Hindu nationalist organizations they pinpointed as key drivers of mass Islamophobia, the RSS and the Bajrang Dal, and recommended that the latter be banned. But it didn’t happen, as the company worried that removing the Bajrang Dal would anger Modi. The Journal revealed last year that the then-head of Facebook India, Ankhi Das, opposed applying hate speech rules to Hindu nationalists and BJP politicians who aimed to spark violence—perhaps due to the fact that she herself was ideologically sympathetic to the country’s Hindu nationalists. (Das stepped down by October 2020.)

We now know for sure that Facebook was fully aware of the RSS’s anti-Muslim crusade and did nothing to address the root issue. And even with this level of appeasement, Modi and his government kept turning their wrath on Facebook for its belated banning of a few Hindu nationalist figures who advocated for killing Muslims. It didn’t matter that Facebook had also removed fake information pages started by opposition politicians and the Pakistani military; any reprimanding of the BJP crossed the line. This year, Modi’s government has cracked down the hardest it ever has on Facebook and other social networks, forcing them to remove posts unfavorable to the BJP, condemning them for spreading content supposedly offensive to fundamentalist Hindus, and threatening to fully expel them if they don’t follow new, restrictive rules drawn up by the Ministry of Electronics and Information Technology meant to ensure compliance. The message is clear: If Facebook doesn’t follow the BJP’s Hindu nationalist dogma to a T, it can kiss its largest market goodbye.

#### Hindu nationalism causes India-Pakistan nuclear war and global proliferation – extinction.

Manchanda ’21 [Rushali; International Politics @ TCNJ; “The Potential Nuclear Consequences of the Rise of Hindu Nationalism in India”; https://celebration.tcnj.edu/wp-content/uploads/sites/115/2021/04/Manchanda-Rushalia.pdf]

The international implications of a potential nuclear attack by India to Pakistan could change the way the world might go to war, the rise of ideologies contributing to conflict can be extremely detrimental. The rise of nationalism as a means to justify an attack on a neighboring state can create a very scary and terrifying world to reside in. If the rise of Hindu nationalism could cause a nuclear weapon to be used, the possibilities for what other states could justify using their nuclear Arsenal on could be limitless. The rise in religious and nationalistic deologies could pave the way for states around the world to start their nuclear proliferation journey. States who are unable to obtain the formula to become equipped when nuclear weapons would suffer tremendously at the hands of those, they might share difficult relationships with their adversaries. This thought makes the future seem bleak and dark, thus why preventative measures must be in place to avoid situations such as this from ever occurring. The implications that surround the potential usage of nuclear weapons by India towards Pakistan are viable and can cause a plethora of changes to the way the international community operates. To prevent the future of the world from seeming so bleak, India must understand the severity of its actions and the implications that surround its need to potentially using its nuclear weapons towards Pakistan.

Conclusion:

The India and Pakistan relationship has been rocky since that time these two states became independent entities. The conflict of both of these states has become one to watch over the years due to its consistent negative trajectory along with the nuclear capabilities of both India and Pakistan. The rise of Hindu nationalism in India has further complicated the situation since it has allowed for this religious ideology to become attached to one of the major parties in the Indian political realm. The Bharatiya Janata Party and Prime Minister Narendra Modi’s Hindutva motivated lawmaking has deeply disturbed the Muslim population within India and the Pakistani government. The changing nature of India's nuclear weapon policy by its Hindu nationalist politicians and military generals has led me to conclude that if the circumstances allowed, India would indeed use nuclear weapons to attack Pakistan. The causal mechanisms in place that would allow a circumstance such as this one to occur would deal with the changes in the Indian public opinion along with the Hindu nationalist tendencies of the Indian media, which is entirely backed by the BJP. The rise and effects of Hindu nationalism in India are dangerous and must be closely examined to prevent a global nuclear catastrophe from occurring.

#### Independently, democracy caps all existential risk.

Eaton ’20 [George; 9/17/20; Senior Online Editor @ New Statesman; Citing Noam Chomsky; Laureate Professor in the Department of Linguistics @ University of Arizona, Professor Emeritus @ MIT, PhD in Linguistics @ UPenn; “Noam Chomsky: The world is at the most dangerous moment in human history”; https://www.newstatesman.com/politics/2020/09/noam-chomsky-the-world-is-at-the-most-dangerous-moment-in-human-history]

Noam Chomsky has warned that the world is at the most dangerous moment in human history owing to the climate crisis, the threat of nuclear war and rising authoritarianism. In an exclusive interview with the New Statesman, the 91-year-old US linguist and activist said that the current perils exceed those of the 1930s.

“There’s been nothing like it in human history,” Chomsky said. “I’m old enough to remember, very vividly, the threat that Nazism could take over much of Eurasia, that was not an idle concern. US military planners did anticipate that the war would end with a US-dominated region and a German-dominated region… But even that, horrible enough, was not like the end of organised human life on Earth, which is what we’re facing.”

Chomsky was interviewed in advance of the first summit of the Progressive International (18-20 September), a new organisation founded by Bernie Sanders, the former US presidential candidate, and Yanis Varoufakis, the former Greek finance minister, to counter right-wing authoritarianism. In an echo of the movement’s slogan “internationalism or extinction”, Chomsky warned: “We’re at an astonishing confluence of very severe crises. The extent of them was illustrated by the last setting of the famous Doomsday Clock. It’s been set every year since the atom bombing, the minute hand has moved forward and back. But last January, they abandoned minutes and moved to seconds to midnight, which means termination. And that was before the scale of the pandemic.”

This shift, Chomsky said, reflected “the growing threat of nuclear war, which is probably more severe than it was during the Cold War. The growing threat of environmental catastrophe, and the third thing that they’ve been picking up for the last few years is the sharp deterioration of democracy, which sounds at first as if it doesn’t belong but it actually does, because the only hope for dealing with the two existential crises, which do threaten extinction, is to deal with them through a vibrant democracy with engaged, informed citizens who are participating in developing programmes to deal with these crises.”

Chomsky added that “[Donald] Trump has accomplished something quite impressive: he’s succeeded in increasing the threat of each of the three dangers. On nuclear weapons, he’s moved to continue, and essentially bring to an end, the dismantling of the arms control regime, which has offered some protection against terminal disaster. He’s greatly increased the development of new, dangerous, more threatening weapons, which means others do so too, which is increasing the threat to all of us.

“On environmental catastrophe, he’s escalated his effort to maximise the use of fossil fuels and to terminate the regulations that somewhat mitigate the effect of the coming disaster if we proceed on our present course.”

“On the deterioration of democracy, it’s become a joke. The executive branch of [the US] government has been completely purged of any dissident voice. Now it’s left with a group of sycophants.”

Chomsky described Trump as the figurehead of a new “reactionary international” consisting of Brazil, India, the UK, Egypt, Israel and Hungary. “In the western hemisphere the leading candidate is [Jair] Bolsonaro’s Brazil, kind of a small-time clone of President Trump. In the Middle East it will be based on the family dictatorships, the most reactionary states in the world. [Abdel al-]Sisi’s Egypt is the worst dictatorship that Egypt has ever had. Israel has moved so far to the right that you need a telescope to see it, it’s about the only country in the world where young people are even more reactionary than adults.”

He added: “[Narendra] Modi is destroying Indian secular democracy, severely repressing the Muslim population, he’s just vastly extended the terrible Indian occupation of Kashmir. In Europe, the leading candidate is [Viktor] Orbán in Hungary, who is creating a proto-fascist state. There are other figures, like [Matteo] Salvini in Italy, who gets his kicks out of watching refugees drown in the Mediterranean.”

# 2AC

## Middleware

### 2AC – AT: Privacy DA

#### Choice turn – consumer choice forces firms to strengthen data privacy protections.

Bennett Cyphers and Cory Doctorow 21. Staff Technologist on the Tech Projects team. Special consultant to the Electronic Frontier Foundation, MIT Media Lab Research Affiliate, visiting professor of computer science at the Open University, visiting professor of practice at the University of North Carolina’s School of Library and Information Science, co-founder of the Open Rights Group. “Privacy Without Monopoly: Data Protection and Interoperability”. EFF. Feb 12 2021. https://www.eff.org/wp/interoperability-and-privacy

This paper focuses on a set of proposals to increase interoperability between dominant companies and their smaller competitors. Interoperability fosters competition, and with competition comes more choice, and the chance to improve the quality of our online lives. An Internet with more competition will allow users to express themselves more freely and craft their online identities more deliberately.

A crucial collateral benefit of interoperability and competition is the potential to improve user privacy. The privacy harms of the tech monopolies are extensive and well-documented. Competition gives users more power to decide how their information is shared and with whom, “vote with their feet” to move to different services when one is not sufficiently respecting their privacy, and chip away at the multifaceted surveillance networks that a handful of large companies deploy. Contrary to major platforms’ assurances, we cannot trust dominant companies to act as unilateral stewards of user privacy. To the extent that companies have to worry about users taking their business elsewhere (especially if users have low switching costs), companies will be pressured to be better stewards.

However, interoperability could cause privacy harms. After all, more interoperability also means companies have new ways to share and collect personal information. This is an argument that the tech monopolies have themselves presented in defense of their behavior, and as part of a promise to behave better in the future. As Mark Zuckerberg has said to the U.S. Congress, “It's not enough to just connect people, we have to make sure that those connections are positive.”

This presents a paradox: market concentration is central to the privacy crisis online, but the path to more competition creates new risks to privacy. One response could be to give up the fight, accept Facebook, Apple, Google et al. as the the best-placed defenders of personal privacy, and regulate them into that role on a presumed permanent basis, as the U.S. did to the Bell System for much of the 20th century.

The goal of this paper is to present a better alternative, one that doesn’t deputize notoriously abusive monopolists to act as a private arm of the state. We can, and should, have both competition and privacy—and users should be able to enjoy the many other benefits of interoperability as well. We treat the risks to user safety and security with appropriate gravity, and argue for a user-centric interoperability policy regime that goes hand-in-hand with privacy.

This whitepaper outlines some EFF proposals to promote competition and innovation through interoperability. It addresses the privacy risks of these proposals and discusses how we can mitigate them and shows why, despite some new risks, interoperability-positive policy does not have to come at the cost of user privacy. Done right, interoperability can actually protect privacy by making it easier for users to control who has their data and how it is used.

#### Market power turn – platforms’ monopolies let them deal the death blow to otherwise-popular privacy laws.

Bennett Cyphers and Cory Doctorow 21. Staff Technologist on the Tech Projects team. Special consultant to the Electronic Frontier Foundation, MIT Media Lab Research Affiliate, visiting professor of computer science at the Open University, visiting professor of practice at the University of North Carolina’s School of Library and Information Science, co-founder of the Open Rights Group. “Privacy Without Monopoly: Data Protection and Interoperability”. EFF. Feb 12 2021. https://www.eff.org/wp/interoperability-and-privacy

2.2. The Status Quo

Though they compete in different markets, most of the tech giants share at least one business model: surveillance. Technology conglomerates collect information about users from each of their dozens of smaller services, synthesize those data into profiles, and use those profiles to target ads. They also gather information about their competitors through app stores and third-party tracking beacons, then target them for acquisition or destruction.

The excessive power of the tech giants has even distorted operating systems and browsers, so that “user agents”—the technical term for web browsers—work more as agents for trackers than for their users. It has warped the priorities of putatively user-centric standards bodies, where seats cost money, participation takes time, time costs more money, and the biggest players control the conversation. It has distorted government policy so that, year after year, privacy laws in the U.S. fail to advance despite overwhelming popular support. The power to achieve all this comes from the tactical weapons that usually correlate to monopoly power: first, they have the excessive profits (“monopoly rents”) that come from the absence of price competition; and second, they are in an industry that is so concentrated that all the major players can agree on how to mobilize that money to secure policies that protect their business.

This practice has come to dominate the technology landscape so thoroughly that other dependent industries find themselves forcibly aligned with the surveillance model. News media companies will draft articles decrying tech surveillance, and then publish them on Web pages loaded with dozens of trackers. Politicians hold hearings on how these tools subvert democracy, even as they pay companies to help them target and track potential voters. Almost every potential champion for digital users ends up on the side of tech surveillance, and against user privacy.

The sadly ironic corollary is that the development of consumer privacy laws in the U.S. has been stunted, so that Internet users' main bulwark against invasive conduct is the large tech companies themselves. For example, after Facebook faced the uproar regarding Cambridge Analytica’s misuse of data collected on its platform, its primary response was to lock down the data it had from third parties, while continuing to collect it for its own use.

The few laws that do protect U.S. users tend to focus on the harms of data sharing and sale, not of the rampant collection and internal processing that Google, Facebook, Amazon, and others perform. These laws are only useful in a world where no single company can document every part of a person’s life.

2.3. The Privacy Paradox

Breaking down the surveillance monopolies by promoting interoperability will help existing privacy laws function as they should. But there’s a catch: policies designed to increase interoperability may weaken the tools that companies currently use to protect their users. To enable tinkering and unsanctioned innovation, we’ll need to dismantle some of the legal weapons that companies brandish and wield against bad actors. In order to mandate baseline levels of interoperability, we’ll deprive companies of their absolute discretion over when they share data and with whom. To the extent that the tech companies are doing a good job shielding users from malicious third parties, users stand to lose some of that protection.

However, one group of users stands to benefit from a reduction in the large companies’ power: those users whose interests are profoundly not served by the tech companies’ protections. These include Uyghurs who want to bypass Apple’s App Store monopoly in order to acquire a VPN that can shield them from the Chinese state; members of rare disease groups on Facebook who are at risk from Facebook’s own data mining; and Google users who attend protests and are at risk from having their location served up to law enforcement agencies with “reverse warrants” seeking retribution.

The policies of large corporations are not—and never were—a good substitute for democratically created and enforced privacy protections. Increased interoperability—and decreased corporate power—opens policy space for real privacy remedies, ones that treat technology users as citizens with rights, not merely as consumers who can make purchase-decisions.

## AT: T

### 2AC – AT: T-Exemptions

#### We meet – patents are an exemption, plan narrows it. That’s Doctorow.

Tejas Narechania 15. Julius Silver Research Fellow, Columbia Law School. “Patent Conflicts”. 103 Geo. L.J. 1483. August 2015. Lexis.

The intersection of patent and antitrust provides familiar terrain for the exploration of patent conflicts. The competing scopes of intellectual property rights and antitrust laws have proved to be fertile grounds for research and legal development, 17 as scholars have long wrestled with the scope of a patent's exception to the antitrust laws. Some have argued that the monopoly grant of a patent is absolute, while others have suggested exclusions that may be enforceable in antitrust. 18 In an important work on this relationship, Louis Kaplow hypothesized the effect of two "extreme doctrinal regimes" that could dictate the resolution of conflict between patent and antitrust. 19 In one, antitrust might "reign supreme," with the practical effect of rendering any action by a patentee that violates antitrust law illegal, regardless of whether the action might be authorized by the patent's right to exclude. 20 Alternatively, patent might be thought to have absolute priority over antitrust, thereby granting a patentee permission to use her patent to engage in anticompetitive behavior, so long as such behavior is within the patent's scope. 21

#### Counterinterp – expand means to increase the scope.

Merriam-Webster ‘ND [“Expand” https://www.merriam-webster.com/dictionary/expand; AS]

2: to increase the extent, number, volume, or scope of : ENLARGE

#### Scope of FTC Section 5 is determined by the FTC.

Joshua Wright 15. FTC Commissioner. “Section 5 Revisited: Time for the FTC to Define the Scope of Its Unfair Methods of Competition Authority”. Symposium on Section 5 of the Federal Trade Commission Act. Feb 26 2015. https://www.ftc.gov/system/files/documents/public\_statements/626811/150226bh\_section\_5\_symposium.pdf

The vague and ambiguous nature of Section 5 is well known. Proposed definitions for what constitutes an “unfair method of competition” have varied substantially over time and belief that the modern FTC has now somehow moved beyond this inherent product of its institutional design are no more than wishful thinking. Indeed, for at least the past twenty years, commissioners from both parties have acknowledged that a principled standard for the application of Section 5 would be a welcome improvement. The lack of institutional commitment to a stable definition of what constitutes an “unfair method of competition” leads to two sources of problematic variation in the agency’s interpretation of Section 5. One is that the agency’s interpretation of the statute in different cases need not be consistent even when the individual Commissioners remain constant. Another is that as the members of the Commission change over time, so does the agency’s Section 5 enforcement policy, leading to wide variations in how the Commission prosecutes “unfair methods of competition” over time. In short, the scope of the Commission’s Section 5 authority today is as broad or as narrow as a majority of commissioners believes it is.

#### Intent to define – this is a table of contents nicety with zero legal meaning. Arbitrary interps incent T over substance.

Christopher Sagers and Anthony Trufanov 21. Sagers is JD and MPP, Michigan. James A. Thomas Distinguished Professor of Law at Cleveland State University. Truf is Truf. “Antitrust Question.” ADT NU Debate. Dec 6 2021. https://nudebateadt.blogspot.com/2021/12/antitrust-question.html

A. What I Really Think

To me, the problem is that this idea of the "scope" of antitrust has no established legal meaning and very little practical significance. It isn't really used in actual practice and it would rarely have any legal significance in an actual antitrust case. It was a convenient shorthand that I came up with for organizing the materials in that book, and it also had one theoretical value to me, but that's pretty much it. Most antitrust lawyers I've worked with understand it what I meant by it, but it doesn't have any precise meaning or doctrinal significance. I don't think the term was even really used before that book. I almost literally made it up.

So, it sounds like participants in this competition are getting hung up on whether particular exclusions from antitrust liability are issues of "scope" or issues of something else, but I don't believe there is any good reason to worry about it. It almost literally doesn't matter, except maybe in the one theoretical sense that I mentioned. (I'll say something about that in a second.) For example, you mentioned this issue of zero-price products, and your students are evidently asking whether the legality of those things should be thought of as involving "limits" on the "scope" of antitrust. But I find myself asking . . . so what? What difference would it make if that is a matter of "scope" or it is something else?

## AT: Regulate CP

### 2AC – AT: Regs CP

#### Perm do both – regulator obviates need for antitrust enforcement. AND, counterplan removes antitrust liability.

Howard Shelanski 18. Professor of Law, Georgetown University; Partner, Davis Polk & Wardwell LLP. “Antitrust and Deregulation”. 127 Yale L.J. 1922. May 2018. Lexis.

The Trinko Court stated that one key factor in deciding whether to recognize an antitrust claim against a regulated firm "is the existence of a regulatory structure designed to deter and remedy anticompetitive harm" because "[w]here such a structure exists, the additional benefit to competition provided by antitrust enforcement will tend to be small." 84 That prudential consideration for precluding antitrust claims against a regulated firm has little to do with whether the plaintiff pleaded a valid antitrust claim or whether that claim could conflict with the regulatory scheme. Indeed, it suggests that even when a plaintiff does plead a cognizable, nonconflicting antitrust claim, courts should still preclude the claim on grounds of enforcement efficiency if a regulatory structure could address the harm. This consideration marked a clear departure from Otter Tail and Gordon, which allowed antitrust intervention even where redundant to existing regulatory authority, absent "plain repugnancy" between the two. By introducing "small additional benefit" as grounds for precluding non-conflicting antitrust claims, the Court potentially undermined the long-standing doctrine favoring antitrust as a complement to regulation. The Court clearly took a skeptical view of such complementarity by finding little benefit from antitrust unless "[t]here is nothing built into the regulatory scheme which performs the antitrust function." 85 The Court thereby suggests that it would displace antitrust if the regulation contains anything that addresses competition, even if it is addressed in only a limited way.

Three years after Trinko, the Court decided Credit Suisse Securities (USA) LLC v. Billing. 86 The plaintiffs in Credit Suisse claimed that the defendants violated Section 1 of the Sherman Act, which prohibits "every contract, combination . . . , or conspiracy, in restraint of trade," 87 by setting securities prices through joint conduct that went beyond what securities laws allow. 88 They also alleged that the defendants had violated antitrust and securities laws by impermissibly engaging in tying and similar activities. 89 Importantly, the Court accepted as given [\*1943] that the securities law did, and "inevitably" would, render defendants' conduct unlawful, so in principle there was no conflict between the antitrust claims and the regulatory statute. 90 The Court nonetheless held that even where a correctly construed antitrust claim would not actually conflict with regulation, the antitrust claim could still be barred on potential conflict grounds. 91 The Court reasoned that "only a fine, complex, detailed line separates activity that the SEC permits or encourages (for which respondents must concede antitrust immunity) from activity that the SEC must (and inevitably will) forbid." 92 Therefore, the Court expanded the notion of plain repugnancy to incorporate not just the genuine conflict that arises when antitrust could bar conduct that regulation might allow, but even conflict between antitrust and regulation that could arise only from judicial mistake or confusion.

Credit Suisse thus went beyond prior implied immunity cases to establish a rule that blocks some claims even when they rely on legitimate antitrust principles, are consistent with securities laws, and, correctly read, would not interfere with the applicable regulatory scheme. Where the underlying conduct is similar enough to regulated conduct that a judge might confuse the two and create a conflict with regulatory authority, the Court chose to err on the side of barring antitrust claims.

The effect of Trinko and Credit Suisse was to render antitrust and regulation more like substitutes and less like complements. The competitive practices, market structure, and market performance of regulated industries are thus more likely to develop without the constraints of antitrust, reflecting instead the potentially different requirements and prohibitions of a regulatory agency's competition-related rules. With antitrust less able to act in parallel or as a complement, the enforcement of competition in regulated industries will depend on the nature of the relevant rules, the agency's commitment to enforcement, and the kinds of sanctions the agency can impose. As agencies repeal such rules or back off from actively administering them, the resulting competition enforcement gap could be greater because antitrust has been sidelined as an available supplement or complement. The doctrinal shift in the relationship between antitrust and regulation that resulted from Trinko and Credit Suisse therefore magnifies the competition enforcement consequences of strong deregulatory cycles.

#### Broad authority – only the FTC has economy-wide investigatory and research authority AND necessary expertise to surveil the entire market for interoperability abuses and capture all anticompetitive practices. That’s Kades. Sector-specific regulators can’t match the FTC.

James Cooper 15. George Mason University School of Law, Director of Research & Policy, Law & Economics Center, and Lecturer in Law. “THE COSTS OF REGULATORY REDUNDANCY: CONSUMER PROTECTION OVERSIGHT OF ONLINE TRAVEL AGENTS AND THE ADVANTAGES OF SOLE FTC JURISDICTION”. 17 N.C. J.L. & Tech. 179. December 2015. Lexis.

IV. THE CASE FOR THE FTC

Not only does efficiency call for eliminating costly duplicative regulation of OTAs, but it also calls for vesting authority with the agency best equipped to handle the task. The evidence suggests that authority should fall to the FTC. First, as explained above, only the FTC has current authority to oversee the entire OTA portfolio of offerings, which allows it to enjoy scope economies in [\*197] enforcement. 74 Second, while DOT's roots are in the regulation of transportation, the FTC has been the nation's consumer protection agency for a century, having developed substantial expertise in advertising generally and online markets, in particular. Third, the FTC's ex-post enforcement-centered approach is far more flexible than DOT's ex-ante rule-based approach. Finally, the FTC's actions are subject to more stringent internal and external checks, and the FTC is less likely to suffer from regulatory capture than DOT.

A. Scope Economies in Enforcement

If moving oversight of OTA airfare offerings from one agency to another merely shifted costs from one agency to another, society should be indifferent between sole or dual jurisdiction over OTAs. This, however, is not the case; resting sole jurisdiction with the FTC is likely to be far less expensive and more effective for taxpayers than shared jurisdiction.

First, leaving aside the relative institutional advantages that the FTC enjoys in this regulatory space (discussed below), sole FTC oversight of OTAs is more cost effective for the simple reason that the FTC can police all OTA offerings at once--something DOT could not perform absent Congressional expansion of its jurisdiction. Second, given the FTC's expertise in e-commerce, scope economies in enforcement means that consolidating OTA oversight with the FTC is likely to reduce total government outlays by almost the entire amount that DOT currently devotes to OTA consumer protection enforcement without any degradation of consumer protection. 75 Indeed, as explained in more detail below, the FTC's expertise and harm-centered approach is likely to improve regulation in this space. Moreover, not only will the FTC's e-commerce experience provide it an advantage in addressing the online sale of air transportation, any experience it [\*198] were to gain from policing the online sale of air transportation would complement the remainder of its enforcement portfolio. 76 For example, the FTC recently addressed the identical issue animating DOT's "full fare advertising" rule. In 2012, the FTC sent letters to 22 hotel operators warning them that failure to disclose resort and other fees associated with hotel bookings on their websites potentially would violate the FTC Act. 77 Although the FTC's warning letters were targeted at hotel operators rather than OTAs, the similarity of the consumer protection issues and industries involved suggest that that the marginal cost for the FTC to address any perceived problems with OTAs' sale of airline tickets would be close to zero.

B. Institutional Competence

The DOT was created in 1966 to oversee the nation's interstate transportation systems: rails, roads, and aviation. 78 Its role with respect to the commercial airline industry was that of traditional utility regulator: through the CAB, it approved pricing, routes, and entry based on a "just and reasonable" standard. 79 Its consumer protection jurisdiction over airline pricing was an artifact of the political compromises involved in airline deregulation, largely due to the fact that FTC lacked jurisdiction over common carriers, including airlines. 80 The legislative history makes clear that the [\*199] consumer protection issues concerning Congress did not involve advertising or other issues related to the sale of airline tickets. 81 Rather, Congress felt that DOT would be in the best position to use the CAB's old consumer protection power to address issues involving airline conduct, such as "overbooking and denied boarding compensation, limitations on liability for lost or damaged baggage, smoking, [and] discrimination against the handicapped." 82 In short, although DOT clearly enjoys substantial expertise in the field of airline safety and industry practice, there is nothing unique about DOT's airline industry expertise that provides it with an advantage in regulating OTA sales of airline tickets. That is, DOT's experience with the airline industry is not likely to enhance its ability to identify practices relating to the sales of tickets that threaten to harm consumers. In economic jargon, because the marginal value of DOT's airline industry expertise to its consumer protection mission is low, the regulatory economies of scope gained by combining consumer protection with other regulatory issues facing airlines are likely quite small. Regulating consumer-facing airline travel displays of OTAs and search engines is light years from the issues that originally led Congress to vest DOT with this consumer protection authority.

On the other hand, the FTC's expertise is not related to one industry, but to consumer protection across all industries; Congress created the FTC to protect consumers from abusive marketplace practices. 83 Its pedigree as the nation's primary enforcer against fraud and deception in advertising since 1938 leaves it with unsurpassed knowledge among regulatory bodies in identifying marketing practices that are likely to harm consumers. 84 In the past year alone, the FTC brought 58 cases involving deceptive [\*200] advertising, 85 held three consumer protection workshops, 86 and issued guidance on a "green" product claim, weight loss claims, and sports equipment concussion protection claims. 87 Moreover, this year the D.C. Circuit in POM Wonderful, LLC v. FTC, noted the FTC's "special expertise in determining what sort of substantiation is necessary to assure that advertising is not deceptive." 88

[\*201] Not only is the FTC the preeminent agency on advertising, it has unique expertise with respect to the Internet economy. As Commissioner Maureen Ohlhausen recently explained, the FTC has consumer protection jurisdiction over the "vast majority of commercial activity on the Internet," and the agency has exercised this jurisdiction to shape norms in online advertising, privacy, and data security. 89 For example, in the early part of the millennium, the FTC used its Section 5 authority to force search engines to more prominently demark paid search results from organic search results. 90 Since the early days of e-commerce, it has used its broad Section 5 authority in an attempt to craft a uniform regulatory approach to privacy and data security concerns. In 1998, the FTC brought its first case against a firm for failing to live up to a promise to care for consumers' data. 91

Since that time, the FTC has brought over 240 cases involving privacy and data security. 92 This enforcement--along with several influential reports--has crafted current U.S. policy on data security and privacy. 93 Additionally, the FTC has been at the forefront of addressing consumer protection issues associated with mobile broadband communications. Last year, for example, the FTC filed [\*202] consumer protection complaints against Google, Apple, and Amazon for failing to disclose purchase windows for in-app purchases. 94 The FTC is also involved in litigation over AT&T's failure to disclose its policy of "throttling" the data of consumers on unlimited data plans. 95

The FTC also has a superior capability to engage in research that informs consumer protection policy. Congress set up the FTC to become a "norm-creator" in large part through studying markets. 96 To help the Commission fulfill this role, Congress gave it the power to subpoena industries for data with which to conduct studies. 97 The FTC has used this power recently to examine privacy issues surrounding data brokers, and currently it is collecting information on patent assertion entities to explore the extent to which their practices give rise to consumer protection concerns. 98 The FTC also conducts several workshops every year, in which it convenes industry experts and leading academics to gather [\*203] information about new issues. These workshops often lead to reports recommending policy or guidance for industry.

For example, in 2009 to 2010, the FTC held a series of workshops throughout the country to solicit opinions on privacy and data security issues. This information gathering resulted in a 2012 report that in many ways operates as a de facto FTC policy statement that guides industry practice in this space. 99 More recently, the FTC released a report on privacy issues surrounding the Internet of Things, based on a workshop of the same name a year ago. 100 Further, its workshop on "Drip Pricing" --the very issues that animated the pricing component of the EAPP-- formed the basis for the group of warning letters sent to hotel operators concerning failure to disclose "resort" or other fees. 101 To summarize, Congress gave the FTC a capability that DOT lacks: the ability to conduct in-depth studies of marketplace practices to create legal norms.

On the whole, the FTC's expertise easily generalizes to the airline industry, whereas it's unclear that expertise in the airline [\*204] industry provides any advantage in addressing consumer protection issues surrounding the online sales of air travel.

#### Internet nascence – Section 5 allows the FTC to update norms and definitions constant as the market changes, which is crucial in an ever-evolving Internet marketplace.

Lisa Jose Fales and Ellen Berge 12. Partner with Venable LLP in Washington D.C.. Of counsel with Venable LLP. “The More Things Change, The MoreThey Stay the Same: Applying Section 5 to Emerging Marketing Practices”. Antitrust, Vol. 27, No. 1, Fall 2012. https://www.venable.com/-/media/files/publications/2012/12/the-more-things-change-the-more-they-stay-the-same/files/applying-section-5-to-emerging-marketing-practices/fileattachment/antitrust\_fall2012\_fales\_berge.pdf

AS TREMENDOUS ADVANCEMENTS in new media and marketing technologies have transformed electronic commerce over the last twenty-five years, the Federal Trade Commission has continued to protect American consumers from fraud with a statutory directive that has remained unchanged since the earliest computers were employed in the late 1930s, back when no one envisioned that computers would be used to sell products and services. The consumer protection prong of Section 5 of the Federal Trade Commission Act, declaring unfair or deceptive acts or practices unlawful, is as deliberately broad and general as the antitrust prong’s prohibition on unfair methods of competition.1 The wording of Section 5 allows the Federal Trade Commission to nimbly adapt its application in the consumer protection context as technologies change and innovative platforms for advertising and marketing emerge, and the Commission has done precisely that.

The last decade has seen an explosion of advertising practices involving new technologies, from cell phones to the Internet. To adapt Section 5 to these ever-evolving practices the FTC can prescribe trade regulation rules identifying the specific acts or practices that constitute a violation of Section 5.2 However, given the stringent requirements of FTC rule- making, the Commission has instead applied Section 5 to these newer practices through strategic enforcement actions, typically resulting in consent orders, and agency guidelines.3 Although these methods have the benefit of being flexible and relatively quick, the downside is that they do not nec- essarily provide clear rules of the road for these new adver- tising mediums.

#### Regulatory capture – regulators are cognitively primed away from stringent enforcement – means the CP inevitably misses some anticompetitive practices.

Sitaraman ’22 [Ganesh; Co-founder and Director of Policy @ Great Democracy Initiative, Professor of Law @ Vanderbilt University; “The Regulation of Foreign Platforms,” *Stanford Law Review* 74 (Forthcoming); AS]

First is the problem of regulatory capture. The technocratic approach assumes that the government regulators who are evaluating companies to determine the necessity of action and a proportional response are not subject to pro-corporate or non-regulatory biases. It is not obvious that this is a sound assumption. There is a well-known revolving door between companies and the federal government,316 and standard theories of capture suggest that government officials from industry—or those who seek to go to industry after government service—will be less likely to stringently enforce regulations against their former or future employers.317 Even if laws were passed preventing the revolving door, regulators often suffer from “cognitive capture.”318 Regulators may have ideological views that cut against regulation (imagine a regulator whose preference is the open internet paradigm) or simply be socialized into an elite community in which they spend time with regulated parties.319 Regulators suffering from these biases would systematically undervalue the necessity of regulation and adopt mitigation measures that are not stringent enough. Note also the interaction with the criticisms above: the more complicated the balancing test or vague the standard, with risk-risk tradeoffs, policy alternatives, and systemic and potential harms, the more discretion regulators will have— and the more space for these biases to shape the outcome.

## AT: States CP

### 2AC – AT: States CP

#### Adaptability – the aff relies on the FTC to constantly update interoperability requirements and act with a unified voice to dictate policy. The CP cannot – process of having the 50 states agree then enforce lacks clarity. Lack of clarity and standardization prevents market entrance – firms don’t know about fiat and perceive legal suicide from interoperating. That’s Doctorow. Getting details wrong worsens anticompetitive practices.

James Mancini 21. Competition Expert at OECD, MSc in Economics from LSE. “Data Portability, Interoperability and Digital Platform Competition”. OECD. 2021. https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

3.2. Risks and limitations of data portability measures in digital platform markets

The term data portability refers to a broad range of functionality and initiatives, ranging from a one-time download of unformatted data provided after a significant delay, to broad, real-time data sharing between digital services using a common API. Thus, the devil is in the details, and the effectiveness of data portability will in large part depend on the context of the market, the design of the measure and the existence of complementary measures. In some situations, data portability may do little to promote competition in digital platform markets, and may even lead to anticompetitive outcomes, in stark contrast to successful applications in other sectors (such as mobile telephone mobility, described above).

#### Patents and copyright – they’re federal defenses to interoperability that state law can’t circumvent – that’s Doctorow. Means the CP gets pre-empted.

Richard Samp 14. Chief Counsel, Washington Legal Foundation. JD from M\*chigan. “The Role of State Antitrust Law in the Aftermath of Actavis”. 15 Minn. J.L. Sci. & Tech. 149. Winter 2014. Lexis, accessed thru Dartmouth.

On the other hand, state antitrust laws--like all state laws--are subject to the restrictions imposed by the Supremacy Clause of the U.S. Constitution, 15 and are impliedly preempted [\*153] to the extent that they conflict with federal law. 16 Such a conflict arises when "compliance with both federal and state regulations is a physical impossibility," 17 or when a state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." 18 On a number of occasions, the Supreme Court has concluded that state antitrust law is preempted because it conflicts with a federal statute other than federal antitrust law. 19

The Court has been particularly quick to find preemption when state antitrust law has an impact on labor law, an area in which federal law is pervasive. 20 Indeed, on at least one occasion, the Court found that a claim arising under state antitrust law was preempted by federal labor law even though the Court concluded that the conduct that gave rise to the state claim could proceed as a claim under federal antitrust law. 21 The Court explained that "Congress and this Court have carefully tailored the antitrust statutes to avoid conflict with the labor policy favoring lawful employee organization, not only by delineating exemptions from antitrust coverage but also by adjusting the scope of the antitrust remedies themselves." 22 The Court said that state antitrust laws "generally have not been subjected to this process of accommodation" and thus that "[t]he use of state antitrust law . . . [must] be pre-empted because it creates a substantial risk of conflict with policies central to federal labor law." 23

Accordingly, in any challenge to a "reverse payment" patent settlement arising under state antitrust law, a court will likely be required to address whether the claim conflicts with the "balance" between federal antitrust law and federal patent law established by the Supreme Court's Actavis [\*154] decision. If such state-law antitrust claims stand as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress in adopting the patent laws, it will be preempted by federal law.

## AT: FTC Tradeoff DA

### 2AC – AT: FTC Privacy DA

#### Khan’s actions now and in the future make actions inevitable.

Okuilar ’21 [Alexander; 7/12/21; Co-Chair @ Morrison & Foerster’s Global Antitrust Law Practice Group, Former Senior DOJ and FTC Official; “FTC Meeting Signals Aggressive and Novel Enforcement to Come”; https://www.mofo.com/resources/insights/210712-ftc-meeting-signals-aggressive.html; AS]

In just over two weeks as chair of the Federal Trade Commission (FTC or “Commission”), Lina Khan already appears to be making significant changes at the agency.[1] As one of her first acts, Chair Khan called for a Commission meeting on Thursday, July 1, 2021 to consider and vote on several important changes to agency rules and procedures, as well as to open several broad investigations. The actions taken at the FTC meeting anticipated the significant Executive Order signed by President Biden last Friday (on which we will shortly send a separate client alert). It was the first public meeting of the FTC in decades (although, it won’t be the last — the FTC just announced another public meeting for July 21) and the matters adopted during the meeting promise to shape the direction of the agency and competition law enforcement in the United States for years. The agenda — published on June 24, 2021[2] — outlined votes on four issues.

Change “Made in the USA” Rules. The Commission’s first order of business was to consider adopting a “Made in the USA” rule imposing civil penalties on marketers making unqualified claims that their products are “Made in the USA” unless 1) final assembly or processing of the product occurs in the United States, 2) all significant processing that goes into the product occurs in the United States, and 3) all or virtually all ingredients or components of the product are made and sourced in the United States.[3]

Remove ALJ as Presiding Officer of Mag-Moss Rulemakings. Next, the Commission debated whether to change Section 18 of the Magnuson-Moss Warranty Act (“Mag-Moss”) rulemaking procedures[4] by 1) making the FTC chair, rather than the chief administrative law judge, the presiding officer, 2) eliminating the requirement of a staff report, and 3) eliminating recommendations as to the final rule for public comment.[5]

Rescind the UMC Policy Statement. Third, the Commission was asked to look at its competition enforcement standards and rescind the 2015 “Statement of Enforcement Principles Regarding ‘Unfair Methods of Competition’ Under Section 5 of the FTC Act” (“UMC Policy Statement”).

Open Industrywide Investigations and Minimize Procedures for Compulsory Process. Finally, the Commission considered whether to open several broad investigations and minimize Commission oversight of compulsory process initiated by career lawyers. The resolutions cut across the economy, including “technology platforms, health care, and pharmaceuticals,” mergers (both proposed and consummated), “repeat offenders” of FTC orders, “business practices that target workers and operators of small business,” and “potential infractions of FTC-administered statutes as they relate to COVID-19.”

In a sometimes contentious meeting, the Commission approved each measure along party lines, with all three Democrats voting in favor and Republicans Christine Wilson and Noah Phillips voting against and offering topping motions that were defeated by the three Democrats. While each of the issues is important, the latter two regarding the rescission of the UMC Policy Statement and the expansion and consolidation of investigative power in the chair have raised a raft of questions among the antitrust community and portend a potentially major departure for the agency in its enforcement approach. We discuss the implications of these competition policy changes below.

Rescinding the 2015 UMC Policy Statement: A Possible Rejection of the Consumer Welfare Standard and Traditional Rule of Reason

The Commission rescinded a bipartisan 2015 UMC Policy Statement that laid out the framework for enforcing Section 5 of the Federal Trade Commission Act. Section 5 makes “unfair methods of competition” unlawful and is the basis by which the FTC brings competition actions.[6] Case law establishes that Section 5 sweeps in conduct condemned by the Sherman Act and Clayton Act, but there is longstanding ambiguity about how far Section 5’s prohibitions extend beyond the Sherman and Clayton Acts. The 2015 UMC Policy Statement contemplated case-by-case Section 5 enforcement “guided by the public policy underlying the antitrust laws, namely the promotion of the consumer welfare standard” using a framework “similar to the rule of reason” requiring evidence of “harm to competition or the competitive process,” including taking into account “cognizable efficiencies and business justifications.”[7] The 2015 UMC Policy Statement was intended to place reasonable bounds on the agency’s ambiguous Section 5 authority and to harmonize its approach to antitrust with that of other government enforcers, private parties, and courts.

Although the 2015 UMC Policy Statement explicitly noted that Section 5 reaches conduct outside the letter of the Sherman Act, [8] Chair Khan criticized it as artificially limiting the scope of the FTC’s authority by tying it to existing antitrust jurisprudence. According to Chair Khan, “coupling Section 5 to the Sherman Act has led courts to bind the FTC to liability standards created by generalist judges in private treble-damages actions under the Sherman Act.”[9] Further, she said, “in practice, the 2015 statement has doubled down on the agency’s longstanding failure to investigate and pursue unfair methods of competition.”[10]

Neither Chair Khan nor any other commissioner supporting rescission has advanced a framework to replace the old 2015 policy. But Chair Khan intimated that the FTC may engage in substantive rulemaking on the matter,[11] stating that “in the coming months, the Commission will consider whether to issue new guidance or to propose rules that will further clarify the types of practices that warrant scrutiny under this provision. In the meantime, the Commission will exercise responsibly its prosecutorial discretion in determining which cases are appropriate under Section 5, consistent with legal precedent.”[12]

Senator Klobuchar praised the move  saying, “We need aggressive action from our antitrust enforcers. Chair Khan has a bold vision for the FTC, and I am encouraged that the Commission is taking steps to use its full legal authority to protect competition.”[13]

Both Republican commissioners opposed rescinding the policy statement.[14] Commissioner Wilson noted that the 2015 UMC Policy Statement was bipartisan, and expressed discontent that it was repealed on a party line vote. She stated that the repeal is an “unfortunate first step” towards a “new concerted effort by the Commission to exceed the FTC’s authority regarding the use of Section 5 of the FTC Act.”[15] Commissioner Phillips also objected to the repeal, arguing that it was unclear what guidance would replace the policy statement and that the decision to rescind without a meaningful opportunity for public input was “inconsistent with the rhetoric” of transparency from Chair Khan.[16]

Rescinding the 2015 UMC Policy Statement has wide ranging and potentially dramatic implications for FTC enforcement under Chair Khan. As a threshold matter, it is consistent with an aggressive, populist neo-Brandeisian view of antitrust that is skeptical of the consumer welfare standard as the cornerstone of competition enforcement. It also shows hostility toward the antitrust laws as interpreted by the federal judiciary. Chair Khan criticized the 2015 UMC Policy Statement as binding the FTC to Sherman Act case law developed by “generalist judges.” Rescinding the policy statement also opens the door to FTC rulemakings for new substantive competition rules. (For a more in-depth discussion of a potential substantive competition rulemaking, see our previous Client Alert.) Finally, it could signal future Robinson-Patman Act enforcement by the FTC. The Robinson-Patman Act prohibits price discrimination, and has been widely criticized as protecting competitors and not competition.[17] While still on the books, neither the FTC nor the U.S. Department of Justice’s Antitrust Division have brought any Robinson-Patman Act enforcement actions in decades.[18] Some neo-Brandeisians have advocated a return to active Robinson-Patman Act enforcement by the federal government,[19] however, and rescinding the 2015 UMC Policy Statement would be consistent with such a return.

Investigations and Enforcement Resolutions

By another 3-2 party-line vote, the Commission approved a series of resolutions authorizing agency staff to investigate and use compulsory process (e.g., civil investigative demands or subpoenas) in seven areas deemed to be “enforcement priorities.” Although the specific resolutions are not publicly available, based on Chair Khan’s remarks and the FTC’s press release, the resolutions appear to cover wide segments of the American economy, including “technology platforms, health care, and pharmaceuticals” and a “general resolution authorizing the use of compulsory process when investigating mergers.” Other resolutions capture investigations involving “repeat offenders,” investigations of “business practices that target workers and operators of small business,” and investigations of “potential infractions of FTC-administered statutes as they relate to COVID-19.”[20] Chair Khan justified the new resolutions as eliminating “extra bureaucratic hurdles [that] slow down and hobble investigations unnecessarily.”[21]

The new procedures will empower staff to issue compulsory process within these broad investigations, including issuing demands for documents and testimony through civil investigative demands (CIDs) and subpoenas,[22] without receiving further authorization from the entire Commission. Under the previous rules, compulsory process in antitrust investigations could only be issued if a majority of the Commission voted to do so, typically on a matter-by-matter basis.[23] After such a vote, individual CIDs could be authorized by the signature of a single commissioner. But under these resolutions, one commissioner now has the power to authorize the use of compulsory process for investigations in the enforcement priority areas. In practice, since the chair directs FTC staff on a day-to-day basis, this will give the chair the unilateral ability to authorize compulsory process without any need to keep other commissioners informed. The “bureaucratic hurdles” that Chair Khan referred to are staff recommendations making the case for compulsory process in a particular matter and the occasional back-and-forth across the Commission pending a vote. These changes could result in less involvement by all commissioners in ongoing investigations, prior to an enforcement decision requiring a full Commission vote.

In opposing the resolutions, Commissioner Phillips argued that they exceed the agency’s congressionally given powers. Phillips observed that “Congress gave the Commission, not a single commissioner or staff, the authority to bless compulsory process in its investigations” because “[i]t envisioned an informed and deliberated decision by all commissioners before unleashing the FTC’s considerable investigative power.” These resolutions “undermine all that,” Phillips observed, “[f]or what are likely to be our most prominent and expensive investigations.” Additionally, Phillips noted that the authorizing language in the resolutions — “unfair, deceptive, anticompetitive, collusive, coercive, predatory, exploitative, or exclusionary acts or practices” — extends beyond the FTC’s authority to investigate “unfair methods of competition . . . and unfair or deceptive acts or practices.”[24] His proposed amendment to conform the authorizing language  to be consistent with the FTC’s statutory mandate was voted down.

Commissioner Wilson argued that the FTC commissioners should not abrogate their authority at such a “critical time for both consumer protection and antitrust enforcement” by removing “significant swaths of Commission oversight from our investigations.” As one practical example of why Commission oversight matters, she observed that, in the past, she had used her “vote on compulsory process to narrow the burden of third parties that are not targets of an investigation.” She flagged that the resolutions contain “many broad and vague terms” and queried whether “authorizing investigations into ‘exploitative,’ ‘collusive,’ ‘coercive,’ or ‘predatory’ acts or practices will lead to investigations outside the bounds of judicially recognized antitrust principles[.]”[25]

Looking Ahead: Further Implications for FTC Enforcement

The adoption of these resolutions signifies an attempt to expand the authority of the FTC and increase the volume and scope of its investigations, particularly for the technology and health care sectors. The Commission majority has signaled its interest in scrutinizing digital platforms, technology companies, pharmaceutical companies, pharmacy benefits managers, and hospitals, among others. Merging parties in key areas of interest (including those with consummated deals) should anticipate more frequent and extensive use of agency process, including inquiries with respect to new or historically less commonly explored theories of harm. Moreover, FTC staff will be more likely to issue compulsory process to third parties. Companies operating in or adjacent to markets in which there are pending mergers or FTC conduct investigations should also be prepared to receive compulsory process, potentially multiple times on distinct investigations that touch on common issues. For better or worse, it is clear from the July 1 meeting that Chair Khan and the Democratic majority on the Commission want the FTC to become a more central feature of corporate life in America. The last time the Commission attempted a similar move in the 1970s, it ended with curtailment of the agency’s powers by Congress and the courts. In her dissenting statement, Commissioner Wilson warned that “there are many at the FTC who lived through the 1970s and 1980s and experienced the public and Congressional backlash during those dark days of the agency’s history. There are many others who worked with and lived through that period. Current management would be wise to seek their guidance.”[26] Only time will tell.

#### Only the aff solves the impact – Interoperability opens data sets to real-time regulation and public pressure – solves AI bias.

Chris Marsden and Rob Nicholls 19. Professor of Internet Law at the University of Sussex, PhD from Essex. Associate professor in regulation and governance at the UNSW Business School, PhD from UNSW. “Interoperability: A solution to regulating AI and social media platforms”. SCL. Sept 19 2019. <https://www.scl.org/articles/10662-interoperability-a-solution-to-regulating-ai-and-social-media-platforms> [acronyms expanded in brackets]

AI is already deployed in ways that we may not even be aware of with incidents of abuse of that data reported daily. In this article, we argue there is a better, broad way to prevent abuse: interoperability. “Computer says no” cannot be the final answer to our quest for justice in such decisions. We argue that what is needed most urgently is a remedy to dominant consumer-facing platforms deploying AI in non-transparent systems. AI is being used in many systems, with little to no transparency, from facial recognition cameras in public spaces to removal of ‘fake news’ from social media platforms, yet consumers have no visibility of these technologies nor remedy if their rights are potentially infringed.In our view the answer is not just a temporary dose of transparency, which may not be feasible or even desirable4, but an interoperability remedy that lets regulators and potential rivals see inside the ‘black box’ to judge the AI for themselves5. There is a caveat: regulation may not be suitable, appropriate or feasible for many algorithms but for those that regulators have most concern about, in sectors that provide the most sensitive socioeconomic decisions, it is a remedy that can be explored. Sensitive public facing sectors may include: banking/credit, insurance, healthcare & medical research, social care, policing and security, education, transport (AI-guided airliners & automated vehicles), social media, telecommunications6. This is a non-exclusive list that may be altered by emerging public techno-socio-policy concerns.

How is AI governed in practice?

At present, AI is largely governed through self-regulation and the technology giants, including the GAFAM/FAANG platform operators7, appear set on persuading us that self-regulation remains the only effective route to legal accountability for machine learning systems. Such an attitude jeopardises the sustainable introduction of smart contracts, permitting algorithmic discrimination and compromising the implementation of privacy law8.

Recent public policy focus on digital decision-making has led to a wider debate about computer-aided adjudication. Legal focus has exposed discrimination that occurs in machine learning parsed into their interaction9. Discriminatory data is likely to lead to discriminatory results. Discriminatory algorithms - as well as those not designed to filter out discrimination - can make those results more discriminatory. Justice requires that lawyers study algorithmic outcomes in order to ascertain such discrimination, which may be highly inefficient as well as outrageous to natural justice and fundamental rights. Public administration has generic solutions. Administrative law requires natural justice, or at least, ‘reasonableness’. A right to explanation and / or remedy should apply, and anti-discrimination law also applies to corporate decisions. AI decision making has raised the question: is the decision maker AI or human?

The case of UK Visa applications demonstrates that AI is not a trustworthy contributor to what was already never a happy or exact science. The UK government minister (at the time of writing) claimed that use of AI in visa applications was acceptable as humans made the final decision: “Sifting is not decision making”10. The Council of Europe in principle disagrees: while to err is human, inducing AI complexity does not absolve the operator of responsibility for harms11.

Our focus in this article is on the private activities of private companies, particularly in networked industries that affect consumers at scale. We now have a variety of pro-consumer/citizen laws that extend rights and obligations far beyond classical freedom of contract, including: anti-discrimination and equality laws; financial regulation; consumer contract law; and telecommunications regulation. Specialist technology law is deployed in many fields that now make up the Information Society: biomedical/nanotechnology deployment; railways, roads, and telecoms; data protection12. Judges may solve problem in tort/contract, though this took 100 years in case of railways litigation, and it would require many technologically savvy judges, and a large number of leading cases in common law jurisdictions to achieve the same outcome. In contrast, the largest civil law system, European Union consumer law, is pressing ahead with legislation to combat AI injustice before the end of 2019, President-elect Von der Leyen stating: “In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence.”13 The new President also promised a new Digital Services Act to regulate large digital platforms. Our proposed solution will approach both issue areas coherently.

Transparency, replicability and general data protection are incomplete solutions to AI

Transparency is the first requirement of legal recourse (though some algorithms can be reverse engineered without transparency “under the hood” of the machine). It is not sufficient, however, for several reasons. Claims that the ability to study an algorithm and its operation provides a remedy for users who suffer as result of decisions falls short for one simple reason: both the training data and the algorithm itself will change constantly. For instance, it is impossible to forecast real time outcomes of Google searches; a vast Search Engine Optimization business attempts approximations without complete accuracy. The only remedy that can be achieved is replicability – taking an ‘old’ algorithm and its data at a previous point in time to demonstrate whether the algorithm and data became discriminatory. This is an incomplete a remedy as it in effect it uses a ‘slow motion replay’ while the game rushes onwards.

Wagner argues for the need for systematic redress by an external agency to instil confidence in AI decision making14. He uses AI deployment case studies to illustrate the point: self-driving cars, police searches using social media/Passenger Name Records, Facebook content moderation. All require minimal regulation for the public to get some trust in using these technologies (some of which are compulsory to use services or even enter countries). ‘Ethics washing’ is undertaken by technology companies and their professional advisors, where attempts are made to persuade policy makers that self-regulation is the only effective route to legal accountability for Machine Learning systems15. If this means the public distrusts AI and any system claiming to use AI, it may be jeopardizing the sustainable introduction of smart contracts, permitting algorithmic discrimination and compromising implementation of data protection law. Regulators are wise to these tricks. Ethics washing will fail16. Cursory research into history of communications regulation and Internet law demonstrates the falsity of this self-regulation proposition17.

The EU right to data portability (“RTDP”) under the GDPR18 might be seen as a partial solution to combat market concentration in EU. The current version of RTDP might be too limited, as portability only applies when the data subject herself provided the data, yet data is often a shared service with multiple owners and creators (consider a selfie photo of best friends, posted by both online in separate accounts with separate tags and hashtags). Further, it cannot be a general instrument of economic policy in digital markets, as data is “unlocked” solely if the data subject invokes RTDP under GDPR.19Edwards and Veale indicate RTDP is not enough and “regulation to promote true interoperability is vital”.20

Competition or communications/media regulation: What can and should be done?

Interoperability enables more free data flow, an essential but not sufficient input for data-driven innovation21. Open and interoperable standards can help to increase competition in digital markets. UK’s Open Banking Standards, designed to enhance competition in the banking sector by enabling fintech entrepreneurs entry to market, could be an appropriate example.22 However, interoperability will not always leads to more innovation and competition.23 Interoperability through uniform standards and interfaces, might limit companies development of their own innovative goods and services with specific components since they have to comply with the requirements of interoperability.24 Implementation of a maximum level of interoperability could also cause privacy harms. If technical and consumer control mechanisms are not well designed, interoperability might increase the risk of misuse of personal data due to multiple service providers access to user’s personal data. Therefore, open and interoperable standards should avoid overstandardization and serve pro-competitive goals.25

We therefore suggest three regulatory options for consumer-deployed AI regulation, though we only propose two should be made operational.

1. Ethical standards for all AI deployed in the ‘wild’ to the public. ISO standards should be implemented with basic privacy/human rights impact assessment.

2. Interoperability for public communications providers – Instant Messaging/Search/Social Media companies

3. API (Application Programming Interface) opened to dominant (Significant Market Power: SMP) operators. This is based on Microsoft remedies in longest, most expensive antitrust case in EC history: a case which started in 1993 and whose remedies, imposed in 2004, only expired at the end of 2014. The later Google antitrust case, started in 2009, is ongoing a decade later26.

Ethical standards for all AI deployed in ‘wild’ – to public

An industry standard could be a baseline for deploying sensitive technologies with cybersecurity and human rights impacts. ISO standards are being formed, and can be quite powerful influencers (see ISO27001 on cybersecurity for example). Typically technical engineering is a realm not considered suitable for normative standards.

However standards embedded in national laws can become a weak coregulatory signal. Basic privacy/human rights impact assessment has been proposed by UN Rapporteur Prof. David Kaye, and AI impact assessment suggested by Mantelero for the Council of Europe27. Standards Australia is chairing an ISO Working Party28.

More broadly, ethics standards for AI deployment have been suggested by many organisations. The European Union29 & OECD Guidelines may receive the widest acceptance30. Many other guidelines exist, such as: the US 2019 Executive Order on AI; UK Centre for Data Ethics and Innovation (CDEI) at Turing Institute31. Hosanagar advocates the creation of an independent Algorithmic Safety Board, modelled on the Federal Reserve Board32.

Why interoperate?

Connectivity and communication are an essential part of contemporary life whether it be individuals using social media or telecommunications, businesses interacting with one another or across government departments. Interoperability at its most basic level can be defined as the ‘ability of two or more systems or components to exchange information and to use the information that has been exchanged.’33

Interoperation is driven by economics: there is nothing less valuable than a network with one user. Interoperability results in increased value of several networks and promotes efficient investment in and use of infrastructure. It permits new entrants to compete with existing operators and promotes entry. Network effects of interoperability are based on a heuristic called Metcalfe's law. Metcalfe hypothesised that while the cost for the network to grow the number of connections is linear, its value would be proportional to the square of the number of users.34 The users and operators of each network gain according to more users of that network, and lose where users switch away to a more popular network.

There are social benefits of interoperability. It eliminates the consumer need to acquire access to every network or the tendency to a winner-takes-all outcome. This is inelegant from a device design perspective too: readers may remember when the US had different mobile design standards to the EU (CDMA rather than GSM). In Instant Messaging (IM), arguably the winner-takes-all is Facebook/WhatsApp/Instagram without interoperability – with all IMs inside the corporation becoming interoperable35.

Interoperability can be divided into technical or non-technical. Technical interoperability includes communications, electronic, application, and multi-database interoperability whilst non-technical interoperability includes organisational, operational, process, cultural and coalition interoperability.

Regulatory intervention can be applied to either but addressing the technological aspects of interoperability provides predictable regulation.

Interoperability option for public communications providers (PCPs)

Interoperability is not radical as a regulatory requirement. It is required for broadcasters to enable Electronic Programme Guides (EPGs), and telecoms companies for telephone numbering schemes. Co-regulatory standards are often used. A PCP interoperability proposal would not regulate public communications providers as utilities but as media providers, and this is not common carrier regulation nor equivalent to energy/postal providers. It is intended to regulate operators as printers, not publishers, with primary content liability remaining with individual user/authors. We note that attempts to impose ‘Duty of Care’ fiduciary in the UK and the US are highly inappropriate and anomalous to the entire history of Internet and analogue free speech and content regulation36.

Not all PCPs will wish to interoperate, not least because the large platform PCPs have been found to have insecure communications and compromised protocols, so smaller PCPs may refuse to interoperate even were the option available. A good example is data security and minimalization philosophy deployed by the founder of Signal (Cryptographer and Open Whisper Systems founder Moxie Marlinspike), a perspective that is shared in part by Telegram37. The PCP interoperability option can therefore only be adopted towards specific dominant operators, not all PCPs, without compromising cybersecurity innovation and the freedom of choice of individual users.

Opening Dominant operators’ APIs

Opening up the API enables brokers, comparator programmes, regulators to access algorithms in real time & controlled conditions, in order to observe the algorithm’s behaviour. Where an operator is found to be dominant, interoperability could be applied as a consumer remedy, not a competition one. EU Commissioner Vestager recently described her policy on interoperability and large platforms:

“Making sure that products made by one company will work properly with those made by others – can be vital to keep markets open for competition. Microsoft’s takeover of LinkedIn approval depended on agreement to keep Office working properly, not just with LinkedIn, but also with other professional social networks. The Commission will need to keep a close eye on strategies that undermine interoperability”38.

Recently, in a contested decision, the Australian ACCC found dominance by Facebook and Google39. Interoperability would only apply to platform aspects of their business, for example mobile app stores not Apple or Android phones. Three models have been proposed:

Model 1: Must-carry obligations, as used for regulating EPGs

Model 2: API disclosure requirements, as with Microsoft from EC rulings40.

Model 3: Interconnect requirements, which are applied to telecoms, especially operators with SMP41. Interoperability can be separated into three types, as identified in a recent study for DG Competition42:

Protocol interoperability: this provides the ability of services/products to interconnect technically. It is the ‘usual’ from of interoperability seen in competition policy, as between the Microsoft Windows operating system and the APIs of Internet browsers such as Firefox and Chrome.

Data interoperability: Recalling Mayer-Schonberger/Cukier and their remedy to ‘Big Data’ monopolists in their eponymous book, this would provide a slice of data to competitors43.

Full protocol interoperability, is what telecoms regulators often think of as full interconnection.

In principle, providing access to APIs is likely to be in the best interest of the service provider. That is, the provider gets the same network effect advantage set out above. However, if a service provider with SMP [significant market power] chooses to make an API private, this may represent a barrier to entry. If a service provider with SMP [significant market power] chooses not to make an API available, this may also represent a barrier to entry. If either of these conducts has the potential to substantially lessen competition, then an ex ante access regime to an API is a potential regulatory solution.

The requirements for such an access regime would be consistent with usual practice associated with either essential facilities or bottlenecks in networked industries. However, there will need to be slight differences in the regime, depending on whether access is to an otherwise private API or to an API that was required to be created as part of the ex ante regulation. The regulatory language required to impose the API obligation is similar to that required in telecommunications. The API provider is referred to as the access provider and the person seeking to use the API is referred to as an access seeker. As such, a preliminary stage of the ex ante regulation might well be to have a regime in which an access provider can make a standing API access offer by having either a public or private API to which access is offered on a non-discriminatory basis where the terms and conditions of access are set out in a Standard API Access Agreement (SAAA). The SAAA would form an offer, capable of acceptance by any member of a class of those qualified to become access seekers.

If there is no such SAAA, then the regulatory access obligation would be in the form set out below.

If the access provider has an API, then the access provider must, if requested to do so by an access seeker:

(a) supply access to the API to the access seeker;

(b) take all reasonable steps to ensure that the technical and operational quality of the API supplied to the access seeker is equivalent to that which the access provider provides to itself; and

(c) take all reasonable steps to ensure that the access seeker receives, in relation to the API, fault detection, handling and rectification of a technical and operational quality and timing that is equivalent to that which the access provider provides to itself.

If the access provider has created an API, then the access provider must, if requested to do so by an access seeker:

(a) supply access to the API to the access seeker; and

(b) take all reasonable steps to ensure that the access seeker receives, in relation to the API, equivalent technical, operational and data access outcomes to those that the access provider provides to itself.

The price of access to an API would usually be based on a building block model approach. In any case, it should return a normal profit to the access provider based on that access provider’s weighted cost of capital. There may be a requirement to provide a safety net set of non-price access terms and conditions in the absence of a SAAA.

Conclusion From Interoperability for Social Media Platforms Deploying AI to Broader Remedy?

We have explained in this article that AI is too dynamic an environment for transparency and replicability to provide a comprehensive solution for users who have suffered injustices. To really help the regulatory environment work in the public interest, we need to introduce interoperability for users and regulators to see ‘inside the black box’ of AI decision makers. Interoperability is not radical as a regulatory requirement and is required for broadcasters and telecoms companies to enable EPGs and telephone numbering schemes respectively. Co-regulatory standards are often used. This proposal would not regulate public communications providers as utilities but as media providers, and this is not common carrier regulation nor equivalent to energy/postal providers. It is intended not to regulate operators as publishers but as printers, with primary content liability remaining with individual user/authors. We are agnostic as to the location of an ‘interoperability regulator’ beyond noting that the deployment of AI is predicted to become so widespread throughout socio-economic arenas that a generic regulator may rapidly be more useful than a communications specific regulator. More research is needed as to whether ‘Ofcom’ should be supplanted or supplemented by ‘OffData’44.

Many research questions for digital competition remain. Interoperability is extensively used in sectors with which we are most familiar. Is this interoperability remedy more broadly applicable? Can self-driving vehicles or banking, insurance, medical algorithmic ‘AI’ be regulated using interoperability? It depends on a variety of socio-economic factors. Many sectors have regulators working on ‘regulatory sandpit’ solutions.

#### FTC consumer-oriented privacy action presumes transparency and consumer choice are sufficient. Wrong.

Terrell McSweeny 18. Former FTC Commissioner. “PSYCHOGRAPHICS, PREDICTIVE ANALYTICS, ARTIFICIAL INTELLIGENCE, & BOTS: IS THE FTC KEEPING PACE?”. 2 Geo. L. Tech. Rev. 514. 2018. Lexis.

Traditionally, privacy concerns focused on providing consumers with notice and choice when personal information is collected along with some explanation of how it will be used and by whom. 15 However, this framework does not address the use of personal information by third parties and data brokers who have no direct consumer-facing relationship, 16 nor does it adequately reach unanticipated uses of data as inputs for complex algorithms or by the increasingly powerful platforms that mediate most consumers' Internet experience. Recent revelations regarding the potential role that consumer data played in training sophisticated targeting tools used to manipulate voters underscores the weakness of consumers to adequately anticipate the consequences and risks of sharing data at the time they are using a service. 17 In fact, there is very little evidence that consumers understand how their data are being used to curate their online experience. 18 And they may be manipulated by the choices they are offered. 19 Moreover, there is little incentive for companies to adopt more privacy- and security-protective designs. 20 As Woodrow Hartzog points out, "The value of personal data has led most companies to adopt a 'collect first, ask questions later' mentality. This mentality incentivizes design choices that marginalize users' interests in opacity and controls over how their data is collected and used." 21

Against this backdrop, the FTC advocated for more consumer-oriented policies in design. But repeated failures by Congress to strengthen the agency have left it with little choice but to continue to pursue an incremental, case-by-case approach focused on protecting consumer access to correct, non-deceptive information about data collection and use. 22 For example, in August 2017, Uber Technologies, Inc., agreed to settle charges that the company falsely claimed that it strictly prohibited its own employees from accessing rider data and monitored internal access to such information. 23 Further, the FTC alleged that the company deceptively claimed that it provided reasonable security for rider and driver's personal information when it actually failed to do so; as a result of the company's failures, a file containing personal information pertaining to more than 100,000 Uber drivers was breached. 24 In some cases, the FTC has also used its deception authority to police the design of privacy settings and options. For example, in February 2018, the FTC announced a settlement resolving charges that Venmo, a peer-to-peer payment service now owned by PayPal, Inc., among other things, misled consumers about the extent to which transactions on the platform could be made private. 25 On the platform, users had to navigate multiple settings to prevent participants in their transactions from overriding their choice to make a transaction private. 26 This case builds on other deception cases before it in which the FTC considered whether the design of consumer interfaces were misleading. For example, in a case involving Snapchat, the FTC alleged that consumers were misled into believing messages were ephemeral and would "disappear forever" even though they did not. 27 And, in its first Internet of Things (IoT)-related privacy case, the FTC alleged that VIZIO's "Smarty Interactivity" interface on its smart TVs did not adequately disclose that consumers' precise television viewing activities would be collected and shared with third parties. 28

The FTC has also used its authority to protect consumers from unfair practices in the privacy and security context, though it has used that authority more sparingly. The FTC's first unfairness privacy case was a case in which the company, Gateway, allegedly retroactively changed its privacy policy. Consumers were only offered an opt-out when their data gathered under one set of terms (a promise not to sell it to third parties) was sold to third parties. 29 The FTC made similar allegations against Facebook in a subsequent case, 30 underscoring that a company cannot collect information for a particular stated purpose and unilaterally decide later to use it for a broader purpose without first obtaining affirmative consumer consent. In the privacy and data security context, the FTC has alleged unfairness in the following situations: collecting and using information obtained through a client's website in knowing violation of that client's privacy policy; 31 selling confidential phone records without consent; 32 designing software causing consumers to unwittingly share files publicly; 33 defeating asserted privacy choices by consumers; 34 installing spyware or man-in-the-middle software without notification or consent; 35 selling information to businesses using it for fraud; 36 unfair tracking (collecting and sharing sensitive data without consumers' consent); 37 revenge porn; 38 and failure to maintain reasonable security practices. 39

The FTC has pursued approximately 40 privacy and security cases in the last decade using its unfairness authority--the majority involving unreasonable data security practices. 40 However, a close examination of these cases reveals that the FTC uses its unfairness authority cautiously in data privacy and security cases. While FTC enforcement can help police the most pernicious and deceptive practices in the marketplace, the agency must develop a clear theory of substantial likelihood of harm to consumers that is not outweighed by any countervailing benefits when using its unfairness authority. 41 The harm requirement imposes some limitations around how far the FTC can pursue aggressive uses of sensitive data. 42 Harms--particularly data harms--are "often remote, diffuse, risk oriented, or difficult to ascertain." 43 As Chris Hoofnagle explains, "So far, the thin edge of the unfairness wedge has been used to police noxious problems such as cyber exploitation, also termed revenge pornography, and spyware." 44 For the most part, the FTC continues to rely primarily on its deception authority when policing consumer privacy and the use of consumer data.

The FTC itself has noted that, especially in light of consumers' ever-expanding connectedness, consumers need additional protections. The agency has repeatedly called for baseline privacy and data security legislation that would be flexible and technology-neutral but would also require breach notification and provide clear rules of the road for companies regarding when they must provide privacy notices to consumers and offer choices about data collection and use. 45

In its 2014 report on data brokers, the FTC highlighted the complex ecosystem of data broker firms, which not only collect data from numerous sources--largely without consumers' knowledge--but also provides data to each other and make inferences about consumers. The edata they collect includes sensitive categories pertaining to income level, ethnicity, or health conditions. 46 The FTC enforces the Fair Credit Report Act ("FCRA"), which covers the use of consumer data for decisions about credit, employment, housing, and similar eligibility determinations. 47 But the FCRA "generally does not cover the sale of consumer data for marketing and other purposes." 48 The FTC identified potential risks to consumers from some of the uses of consumer data and profiles by data brokers. For example, the report noted that storing massive amounts of data may expose consumers to security risks if that information is breached and that risk mitigation and scoring products, i.e., products used to verify consumers' identities or detect fraud, may be used to deny consumers the ability to complete a transaction. 49 To address that gap, the FTC recommended Congress enact legislation that would require data brokers selling marketing products to give consumers access to their data at a reasonable level of detail and to provide the ability to opt out of having it shared for marketing purposes. 50 The agency further recommended that Congress enact transparency obligations on data brokers who sell risk-mitigation products and impose requirements on data brokers selling people search products that would allow consumers to access and suppress their information. 51

The FTC's 2016 report on Big Data examined the benefits and risks of big data analytics, among them the potential to harm consumers, including underserved and low-income populations. 52 The report discussed several laws that could be potentially applicable to the use of big data--including not just the FTC Act but also the FCRA, equal opportunity laws such as the Equal Credit Opportunity Act and Fair Housing Act, and civil rights laws. However, the report noted that determining which law(s) might apply is a fact-specific determination and highlighted the potential for gaps in the enforcement regime.

Congress has shown its willingness to provide the FTC with additional enforcement authority to cabin harmful uses of automated technology or unreasonable limitations on users. Namely, Congress gave the FTC the responsibility to enforce the Consumer Review Fairness Act 53 and the Better Online Ticket Sales ("BOTS") Act, 54 both of which were enacted in late 2016. These laws ban the use of contract provisions that prohibit or penalize consumers who provide honest reviews, and the use of ticket-buying "bots," respectively.

The FTC's enforcement actions are an important basis for the privacy best practices the FTC has endorsed, including: privacy by design, where firms promote consumer privacy throughout their organizations and at every stage of the development of their products and services; 55 security by design; 56 transparency and choice; 57 data minimization; 58 and enhanced protection for sensitive data. 59

But in the data-driven digital economy, the incentive to gather as much data as possible is powerful and often conflicts with these best practices. As Woodrow Hartzog explains, "data is fuel for industry . . . . Manipulative and leaky design can net companies more data. Add to the mix the fact that pernicious design is difficult for people to recognize--it is often opaque and sometimes completely invisible. This is a recipe for exploitation." 60

II. FTC 2.0: CONSUMER PROTECTION FOR THE DIGITAL AGE

The growing power of the technology we are all using in our daily lives--which now includes many more connected and increasingly autonomous things--raises the question of whether consumer protection agencies like the FTC can adapt quickly enough to keep pace with it. As discussed above, the FTC's data protection framework continues to rely heavily on its deception authority and, therefore, the principle that sufficient transparency enables consumers to make informed choices a

bout when to share their data. The idea that privacy controls such as notice and choice are adequate to protect consumers in the current environment has been described as quaint. 61 The FTC has used its unfairness authority to police some data practices, though cautiously and incrementally. Technology is becoming both more powerful and more ingrained in all aspects of our life. Adequately protecting consumers requires a more proactive approach.

One solution is for the FTC to use its unfairness authority more aggressively, and perhaps even its Magnuson-Moss rulemaking authority, to push industry norms toward the best practices that the FTC itself articulates. But this may be easier said than done. Although FTC has used its unfairness authority relatively cautiously, it is constantly called on to defend its use of the authority when it does use it. The FTC won a critical case protecting the use of its unfairness authority in data security cases in Wyndham, but the agency's authority has continued to be the subject of litigation in D-Link and LabMD. 62 In a recent ruling in the LabMD case the 11th Circuit did not directly address the scope of the FTC's unfairness authority -- but nevertheless vacated the FTC's order. 63 In a somewhat unusual move, the court ruled on the appropriateness of the relief sought by the FTC even though the central dispute in the case was over the FTC's use of its unfairness authority. The court concluded that the FTC's order requiring LabMD to implement a reasonable security program was not sufficiently specific. 64 The implications of this decision on future FTC data security cases and efforts by the FTC to enforce existing orders are unclear, but it is likely the decision will result in new challenges to the FTC's authority, particularly in data security cases. In addition, the agency has, historically, run into significant resistance from industry and Congress when it is perceived as pushing the bounds of its authority to expand enforcement efforts innovatively. For example, when the agency attempted to regulate the advertising of sugary foods to children in the late 1970s--actions that resulted in advertisers, broadcasters, and the food industry aligning against the FTC, and in the Washington Post labeling the agency the "National Nanny" 65--Congress stepped in to limit the Commission's authority. The hangover from the so-called "Kidvid" controversy remains a reminder to the FTC today that pushing too aggressively can result in painful consequences.

#### No spillover between consumer protection and competition bureaus.

Spencer Weber Waller 5, Professor of Law and Director of the Institute for Consumer Antitrust Studies at the Loyola University Chicago School of Law, “In Search of Economic Justice: Considering Competition and Consumer Protection Law”, Loyola University Chicago Law Journal, 36 Loy. U. Chi. L.J. 631, Winter 2005, Lexis

Despite this more comprehensive mission, the FTC is organized in a way that tends to emphasize the separation of these fields, rather than the common elements of the agency's mission. The FTC has a Bureau of Competition and a separate Bureau of Consumer Protection, with a Bureau of Economics to support the work of both endeavors. The Bureau of Competition ("BC") primarily engages in the investigation and enforcement of mergers and complex civil antitrust cases with a recent emphasis on intellectual property and health care issues. The Bureau of Consumer Protection ("BCP") primarily investigates and challenges outright fraudulent conduct. 9 The FTC website details recent BCP activity involving Internet sales, telemarketing, false health and fitness claims, identity theft and similar issues. 10 These are all very different issues from the day-to-day focus of the competition staff. This basic split is further mirrored in the Bureau of Economics ("BE"), where the staff tends to specialize in either competition or consumer protection. Any crossover of staff and cooperation occurs primarily in competition advocacy before legislatures or regulatory agencies, and not in case selection and investigation.

#### Rulemaking frees resources.

Chopra & Khan ’20 [Rohit; Commissioner @ Federal Trade Commission; and Lina; Chairperson @ Federal Trade Commission, JD @ Yale Law School; “The Case for “Unfair Methods of Competition” Rulemaking,” *The University of Chicago Law Review* *87*(2), p. 357-380; AS]

Second, establishing rules could help relieve antitrust enforcement of steep costs and prolonged trials. Identifying ex ante what types of conduct constitute “unfair method[s] of competition” would obviate the need to establish the same exclusively through ex post, case-by-case adjudication. Targeting conduct through rulemaking, rather than adjudication, would likely lessen the burden of expert fees or protracted litigation, potentially saving significant resources on a present-value basis.47

## AT: Biz Con DA

### 2AC – AT: Biz Con DA

#### Not unique AND short-term shocks are inevitable – COVID, 08, and daily swings in the market disprove that data blips meaningfully affect sustained economic vitality.

Friedman 21 – Zack Friedman, senior contributor to Frobes, citing Dartmouth econ prof David Blanchflower, “Is The U.S. Already In A Recession?” 10/21/21, https://www.forbes.com/sites/zackfriedman/2021/10/21/research-us-already-in-recession-that-could-be-as-bad-as-2008/?sh=6c6fb48068eb

The U.S. is already in a recession that could be as bad as 2008, according to new research.

Here’s what you need to know.

Economy

David Blanchflower, a Dartmouth professor and former member of the Bank of England Monetary Policy Committee, and Alex Bryson, a University College London professor, claim in new research that the U.S. already entered recession in late 2021. This is contrary to recent economic headlines that promote a soaring stock market and low unemployment data. Based on an analysis of key consumer data, the professors argue that the economic downturn could rival the 2008 financial recession. Here’s why:

Economic crash: reasons why

The professor write that there are several reasons why an economic crash is imminent:

Consumer Data is Ominous

Every recession since the 1980s has been precipitated by a 10-point decrease in consumer confidence indices from the University of Michigan and the Conference Board. In 2021, the Conference Board measured a 25.3-point drop in consumer confidence, while the University of Michigan measured a decline of 18.4 points. In comparison, in advance of the 2008 financial crisis, the Conference Board recorded a 19-point decline and the University of Michigan recorded a 21-point decrease. Blanchflower and Bryson say consumer confidence indices are important because they ask everyday Americans for the views on the economy and expectations about income and employment.

GDP is artificially high

The authors argue that Gross Domestic Product (GDP) in the U.S. is artificially high. They say the real GDP is one year behind what economic data suggests.

Unemployment is artificially low

Record unemployment rates — and a quick recovery from the Covid-19 pandemic — may not tell the entire story. The authors argue that unprecedented government support in terms of unemployment insurance and other economic stimulus has propped up the jobs market, according to the authors.

Economists previously missed these indicators

The authors note that while the data supporting their argument could be wrong, economists dismissed similar indicators in 2007 before the Great Recession.

#### Antitrust inevitbable

Issie Lapowsky 22. Protocol's chief correspondent, covering the intersection of technology, politics, and national affairs. “'Enforcers are not gonna back down': Lina Khan talks rewriting the rules of antitrust”. Protocol. Jan 19 2022. https://www.protocol.com/bulletins/lina-khan-cnbc-interview

In her first TV interview since becoming chair of the Federal Trade Commission, Lina Khan had a message for business executives who think their money, lawyers and lobbyists will shield them from antitrust scrutiny: "Enforcers are not gonna back down."

Over the course of a lengthy CNBC interview Wednesday, Khan expounded on the ways in which she believes antitrust enforcement in America needs to change, a process that is already underway at the FTC. This week, Khan and Jonathan Kanter, the Department of Justice's top antitrust cop, announced a plan to review policies related to mergers, signaling their intention to scrutinize more deals that once flew under the radar.

"The project of potentially revising the guidelines is to basically identify: What are the blind spots right now?" Khan said during Wednesday's interview.

She went on to explain why she thinks such a review is long overdue, saying that Congress first determined that mergers that "substantially lessen competition or tend to create a monopoly" are illegal back in 1914. "What that means in practice is going to change depending on the economy," she said. "As we've seen, the growth of new technologies, the market dynamics have changed, and so we need to make sure that the tools we're using, the frameworks we're using, the questions that we're asking, are actually still mapping onto the reality."

That reality, Khan argued, includes massive digital operations that offer their services for free, but often cost consumers their privacy. Those kinds of harms — see also, labor harms and quality degradation — haven't traditionally factored into antitrust discussions, which have focused primarily on whether companies are using their market power to raise prices. Khan said she wants to refocus enforcers' attention on a broader spectrum of harm, and pointed to the FTC's recently amended case against Facebook (now Meta) as evidence of that approach. Earlier this month, a federal judge allowed the complaint to proceed.

"There was an important discussion in that opinion around the ways in which the courts can understand non-price harms," Khan said Wednesday. "Certain types of quality degradation, certain types of harms to privacy, those could be recognized as harms, even if you're not seeing an increase in the dollar price that people are are paying."

Even as this new approach potentially broadens the scope of enforcement actions the FTC could take, however, Khan noted that the commission is as constrained as it's ever been in terms of funding. "We are severely under-resourced," she said.

That means that the FTC will continue to have to prioritize certain cases over others. Khan said cases that stand to have a deterrence effect or an impact on a broader market beyond a single company will be a top priority. So will cases involving "intermediaries or companies that may be facilitating bad practices going upstream," Khan said. Khan emphasized that this work will not be exclusive to the tech industry, despite her well-known reputation as a tech critic, particularly when it comes to Amazon. And she said enforcement may also need to apply retroactively to deals that didn't get adequate scrutiny the first time around.

#### No shock – firms want interoperability because of upstream benefits of aggregating user data.

Chinmayi Sharma 19. JD, UVA Law. “Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability”. 50 U. Mem. L. Rev. 441. Winter 2019. Lexis. Gendered language [corrected].

The symbiotic relationships fostered by APIs enhances competition in the digital marketplace. Interoperability can have three types of effects on competitive markets:

(1) Direct, in which increased use increases the value of the product itself; (2) indirect, in which increased use leads to development of complementary products, such as applications for a specific platform, which in turn increases the value of the product; and (3) two-sided, in which increased use by one set of users increases the value of a complementary product and vice-versa. 44

Economists widely recognize the formidable hurdle of entering online markets as a feat that "requires either building up strong brand recognition to draw users to an independent site," a resource intensive route, "or using an existing platform," 45 an option made possible by permissive APIs. Innovative products and new startups built off existing platforms use permissive APIs to gain a foothold in a tumultuous market. In turn, the original platforms increase in value and experience an influx of new users. As the saying goes, "rising tides raise all ships."

Interoperability also lowers the barrier of entry to the online marketplace by encouraging the development of complementary platforms. 46At the early stages of the Internet, online platforms were united in their pursuit for active, loyal user bases and collaborated with [\*454] each other to accomplish these goals. 47APIs helped broker these cooperative, pro-competitive strategies. For example, Instagram has witnessed the advent of Instagram celebrities, or individuals who appear to have accumulated overnight fandom teaching people to "be yourself." 48In reality, they are the success stories of third-party apps that allow for planned posts, 49follower analytics, 50and trend-worthy Boomerangs. 51These third-party apps rely on Instagram's API to pull information about users and push information such as curated content. Instagram and these third-party apps mutually benefit from the traffic generated. Security apps have also flourished because platforms like Instagram are reliant on them, 52recognizing platforms sink when users feel unsafe.

The pro-competitive benefits of this "rising tides raise all ships" approach to API design extend beyond encouraging the development of complementary products. Platforms with more universally beneficial services or information can offer access to their APIs for a fee. 53 [\*455] This type of open access to platforms allows for more options to flood the market, theoretically driving out poor quality options that are unable to generate sufficient value to bear the cost of using the API. For example, Google provides its Maps product to developers at a price based on use. 54This allows developers to put Google Maps on their websites and enables users to get directions to a location directly from their app without going to Google. 55The developer pays for this use at a cost proportional to the traffic his or her [their] third-party product generates. 56 This has created an economy of map-based applications that detect potholes, warn of anomalous traffic, and suggest new restaurants, without the new companies having to recreate Google Maps from the ground up. 57

#### No impact.

**Walt 20** – Stephen Walt, International Relations Professor at Harvard University. [Will a Global Depression Trigger Another World War? 5-13-20, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-depression-economy-world-war/]

On balance, however, I do not think that even the extraordinary economic conditions we are witnessing today are going to have much impact on **the likelihood of war**. Why? First of all, if depressions were a powerful cause of war, there would be **a lot more of the latter**. To take one example, the United States has suffered **40 or more recessions** since the country was founded, yet it has fought **perhaps 20 interstate wars**, most of them **unrelated** to the state of the economy. To paraphrase the economist Paul Samuelson’s famous quip about the stock market, if recessions were a powerful cause of war, they would have predicted “nine out of the last five (or fewer).”

Second, states do not start wars unless they believe they will win a quick and relatively cheap victory. As John Mearsheimer showed in his classic book Conventional Deterrence, national leaders **avoid** war when they are convinced it will be **long**, **bloody**, **costly**, and **uncertain**. To choose war, political leaders have to convince themselves they can either win a quick, cheap, and decisive victory or achieve some limited objective at low cost. Europe went to war in 1914 with each side believing it would win a rapid and easy victory, and Nazi Germany developed the strategy of blitzkrieg in order to subdue its foes as quickly and cheaply as possible. Iraq attacked Iran in 1980 because Saddam believed the Islamic Republic was in disarray and would be easy to defeat, and George W. Bush invaded Iraq in 2003 convinced the war would be short, successful, and pay for itself.

The fact that each of these leaders miscalculated badly does not alter the main point: No matter what a country’s economic condition might be, its leaders will **not** go to war unless they think they can do so **quickly**, **cheaply**, and with **a reasonable probability of success**.

Third, and most important, the primary motivation for most wars is the desire for **security, not economic gain**. For this reason, the odds of war increase when states believe the long-term balance of power may be shifting against them, when they are convinced that adversaries are unalterably hostile and cannot be accommodated, and when they are confident they can reverse the unfavorable trends and establish a secure position if they act now. The historian A.J.P. Taylor once observed that “every war between Great Powers [between 1848 and 1918] … started as **a preventive war**, not as **a war of conquest**,” and that remains true of most wars fought since then.

The bottom line: Economic conditions (i.e., a depression) may affect the broader political environment in which decisions for war or peace are made, but they are **only one** factor among **many** and **rarely the most significant**. Even if the COVID-19 pandemic has large, lasting, and negative effects on the world economy—as seems quite likely—it is **not likely** to affect **the probability of war very much**, especially in the short term.

#### New merger guidelines kill biz con

Feiner 1/18 – Lauren Feiner, tech policy reporter at CNBC, “FTC, DOJ seek to rewrite merger guidelines, signaling a tougher look at large deals,” 1/18/22, https://www.cnbc.com/2022/01/18/ftc-doj-seek-to-rewrite-merger-guidelines.html

Now, with both Kanter and Khan in place, the agencies are embarking on a potential overhaul of existing guidelines for businesses seeking to close deals. It comes amid a surge in mergers that has overwhelmed the under-resourced agencies and led the FTC to take unusual steps, like warning some businesses that it will continue to look into their deals after the period of time the parties are required to wait to close.

Kanter made clear that the two agencies are aligned in their approach.

“Way too much has been made of the purported divergence between the DOJ and the FTC on the treatment of vertical mergers,” Kanter said. “The Antitrust Division shares the FTC’s substantive concerns regarding the vertical merger guidelines. Those guidelines overstate the potential efficiencies of vertical mergers and fail to identify important but relevant theories of harm.”

While ultimately any deals the agencies choose to challenge will be up to a court to decide whether to block or allow to close, increased deal scrutiny has the potential to ward off some deals that businesses simply feel are more trouble than they’re worth. Some deals come with hefty breakup fees should they not close, for example, which some businesses may be more hesitant to take on should the risks to closing on time pile up. Still, some antitrust experts believe businesses are likely to continue to push ahead with deals they feel are truly strategic.

#### “Shocks” are inevitable and have no impact.

Bagrie ’18 [Cameron; 8/9/18; Managing Director @ Bagrie Economics; “Business Confidence Is a Hopeless Indicator. But That Doesn’t Mean the Economy Isn’t in Trouble”; https://thespinoff.co.nz/business/09-08-2018/business-confidence-is-bullshit-but-that-doesnt-mean-the-economy-isnt-in-trouble]

The good news is that business confidence is hopeless as an economic indicator. The correlation with economic growth is poor and I largely ignore business confidence readings. Changes in direction can provide some insightful information – whether things are picking up or slowing down, but not the levels.

Businesses tend to be more upbeat regarding general confidence about the economy under a blue flag as opposed to a red one. Business confidence averaged minus 18 between 2000 and 2007. The economy (measured by real gross domestic product) grew on average by more than 3.5% per year. Yep, confidence was negative, but growth was positive. So, we ignore business confidence as an economic indicator. This is nothing new. It’s surprising headline business confidence figures receive so much attention.

Commentators make the constant mistake of saying the ANZ survey is a business confidence survey. The same applies to the NZIER’s QSBO. They are surveys of business views across an array of key indicators including prospects for growth, hiring, whether firms are planning to invest and experiences with inflation / costs. These indicators matter. Business confidence is one question.

The so-called “soft” or “perception” indicators are the hard data of tomorrow. They are estimates and view based but you can’t ignore them. They are well correlated with growth.

In a perfect world we’d have timely “hard” official data and statistics. We don’t. Official data comes with a lag. So, we need to rely on sentiment-based indicators if we want timely readings on the economy and a guide as to the year ahead.

The likes of the ANZ survey are showing a sombre mood when it comes to indicators that matter. The ANZ survey asks key questions about activity, employment, investment and profitability. When these indicators head to zero, which they have done now, growth can do the same. Those indicators were weak in 2000 during the so-called winter of discontent – and growth slowed to 0.9% year on year.

Growth did rebound. But back then the economy was early in the economic expansion. The economy is late in the business cycle this time around. The economy has tended to go through a ten-year cycle, so businesses are naturally looking more nervously over their shoulders at present. The economy is going through substantial economic change too and businesses are wary. There is little argument over the need to change the economy. However, there are serious questions about the actual economic plan and what the new economy looks like. That is a key issue that needs addressed.

Some of the weakness in survey measures could be put down to the way survey questions are phrased. Firms are asked their view and given three options; will conditions improve, stay the same, or worsen. For a lot of firms’ things are damned good. It’s telling that finding skilled staff is the biggest problem firms are facing. Businesses are facing capacity constraints. So, zero readings may reflect a levelling out at a high base.

## AT: Politics

### 2AC – AT: Politics DA

#### Seriously “dead”

Richard Kessler, Editor at Recharge, 2-2-22, "'No. It's dead'," Recharge | Latest renewable energy news, https://www.rechargenews.com/energy-transition/no-its-dead-us-climate-bill-holdout-manchin-gives-grim-judgment-of-prospects/2-1-1162167

US President Joe Biden’s signature $2trn Build Back Better bill, which partly aimed at reasserting US leadership on climate action, is “dead” and Democrats in Congress should start addressing other pressing national issues before trying to re-float a scaled back version, senator Joe Manchin, the key swing vote in the Senate, has claimed.

Asked Tuesday by US news outlet CNN as to whether he has had discussions on the legislation – which contains over $500bn in incentives for renewable energy and climate action, including incentives aimed at overcoming bottlenecks in development the offshore wind sector’s supply chain, port infrastructure, and transmission – the West Virginia Democrat said, “No, no, no. It’s dead.”

When pressed about supporting a smaller package, he added: “We’ll see what people come up with. I don’t know.”

In December, the politically moderate Manchin announced he would oppose the partisan mammoth bill as written after months of personal lobbying by Biden and intense pressure from the party’s ascendant left flank, effectively killing it in the evenly divided 100-seat Senate.

With Republicans against, Democrats with Biden’s support adopted a strategy to win passage with a simple majority of 51 using a legislative manoeuvre called ‘reconciliation’ instead of the usual 60 votes required for major bills.

That gambit hinged on support from all 50 Democratic senators and then-vice president Kamala Harris in her role as president of the Senate casting the deciding affirmative vote. In November, the House of Representatives where Democrats have a thin majority, narrowly passed its version of the bill.

Manchin expressed deep reservations about the cost and scope of the bill, which also seeks to revamp the country’s education, healthcare, immigration, and tax laws, even after it was downsized several times from the initial $3.5trn sought by Biden.

Instead of formulating a massive spending bill, he wants Congress and the White House to first develop a more effective national response to Covid-19, which has now claimed over 900,000 Americans’ lives, and take aggressive actions to slow inflation currently at a four-decade high.

#### Biden publicly supported antitrust legislation this week- zero da

Bordelon 2-4-22

(Brendan, https://www.politico.com/newsletters/morning-tech/2022/02/04/under-pressure-biden-backs-antitrust-push-00005579)

WHITE HOUSE GETS OFF THE FENCE — The Biden team came out in favor of the antitrust measures moving through both houses of Congress late Thursday — but how much public support and political capital the White House aims to spend on reining in giant tech companies remains an open question. The move, coming hours after the Senate Judiciary Committee advanced a bill to break Apple and Google’s hold on app stores, marks the first time the White House has officially weighed in on the congressional antitrust push, Leah and POLITICO’s Adam Cancryn reported. While the White House held a “listening session” with supporters of tech antitrust reform two weeks ago, it offered a neutral readout afterward, saying only that officials “look forward to working with Congress to make bipartisan progress on the issue.” But that polite restraint ended this week following the administration’s foray into the European Union’s draft Digital Markets Act — a package of rules designed to rein in the power of tech giants. As Leah and POLITICO EU’s Samuel Stolton and Mark Scott reported, D.C. antitrust advocates weren’t pleased with the policy paper, thinking it could undermine pending congressional legislation targeting the digital giants. The Transatlantic Consumer Dialogue — a group of 75 U.S. and EU consumer groups — called out the Biden administration Thursday for expressing “concern” about the administration’s statements on the DMA. “The DMA does not target U.S. companies but rather targets companies that are in a position to define how goods, services, and information reach customers and which too often turn this position to their advantage to the detriment of competition and consumers’ interests,” the groups said, urging Biden to “work constructively with the EU” on finalizing the legislation. Biden was always going to have to make a decision on whether to publicly back the antitrust bills — particularly with congressional Democrats split. About those intraparty tensions … The moderate House New Democrats met Thursday afternoon with antitrust chair David Cicilline (D-R.I.) to talk about the tech antitrust bills. (Leah and Emily with the report.) Aides said the meeting was polite, but at least one member — Rep. Suzan DelBene (D-Wash.) — expressed serious concerns. The 97-member coalition will meet next week with two other vocal opponents, California Democrats Zoe Lofgren and Lou Correa.

#### New appointment thumps every link- Focus, PC, floor time

The Hill 1-31-22 https://thehill.com/homenews/administration/591883-breyer-retirement-latest-complication-for-biden-spending-bill

Supreme Court Justice Stephen Breyer’s plans to retire have thrown another curveball into the winding efforts to get the cornerstone of President Biden’s agenda passed in what could be the final months Democrats have full control of Congress. Appointing Breyer’s replacement to the court is an undeniable win for Biden and the Democrats, some of whom had pleaded for the 83-year-old justice to step down and make way for a younger judge to cement the liberal wing of the bench. But the timing of the announcement, nine months before the midterm elections, could make it more difficult for Biden and Democratic leaders to negotiate and get his signature climate and social spending proposal, Build Back Better, passed and signed into law. “At some point, that nomination process is going to consume all of the oxygen on Capitol Hill in the Senate,” said Jim Manley, a former aide to the late Sen. Harry Reid (D-Nev.). “It doesn’t mean Build Back Better is done, but it’s just another problem that has to be dealt with.” Biden said he plans to announce his nominee by the end of February, and Democratic aides indicated that Senate Majority Leader Charles Schumer (D-N.Y.) hopes to follow a confirmation timeline close to that of Supreme Court Justice Amy Coney Barrett, who was confirmed 30 days after she was nominated. A nomination will be followed by confirmation hearings before the Senate Judiciary Committee and eventually a confirmation vote on the Senate floor. While nothing expressly prevents the White House from trying to get the spending package finished before the Supreme Court vote, it will be complicated to do so once Biden unveils his nominee, given the attention the confirmation process will soak up. Democrats desperately want to see a version of Build Back Better passed while they still hold control of both chambers of Congress and the White House. But the bill has run into hurdle after hurdle in the Senate once it passed the House. After months of talks, Sen. Joe Manchin (D-W.Va.) in December said he could not support the legislation and said last week negotiations would be “starting from scratch.” “We have to walk and chew gum at the same time here in the White House,” White House press secretary Jen Psaki told reporters Wednesday when asked whether there were concerns that a Supreme Court nomination process would complicate other legislative priorities, like Build Back Better. “We are entirely capable of doing more than one thing at once.” One Democratic strategist close to the White House argued it was too soon to say for sure if Build Back Better was directly imperiled by the Supreme Court opening. They suggested the confirmation process could provide a win for Biden and Democrats and allow for a cooling off period before returning to negotiations with tensions lowered. ADVERTISEMENT But the strategist acknowledged that getting the Build Back Better bill passed in time for voters to see tangible benefits before the midterms would become more difficult given the confirmation process, and other measures with bipartisan support could push it farther to the backburner. “Time is not the friend of Build Back Better,” said Manley. “The longer this stretches out, the more difficult it’s going to become.”

#### Lujan absence derails Biden agenda

AP 2-3-22 https://apnews.com/article/stephen-breyer-coronavirus-pandemic-joe-biden-us-supreme-court-health-618b25ed7ac76d07fa3a2a1c37b6f161

WASHINGTON (AP) — The Democrats’ fragile hold on the Senate majority became vividly apparent Wednesday with the sudden illness of New Mexico Sen. Ben Ray Luján, who won’t be back to work for at least four weeks, throwing President Joe Biden’s Supreme Court pick and lagging legislative agenda in doubt. The 49-year-old Democrat remained hospitalized after suffering a stroke and is expected to make a full recovery. But Senate colleagues were blindsided by the news — even top-ranking leaders were reportedly unaware that Luján fell ill last Thursday, a stunning oversight. Barring any complications, he is expected to be back at work in four to six weeks, according to a senior aide granted anonymity to discuss the situation. Without Luján’s presence, the party no longer has full day-to-day control of what has been an evenly split Senate, leaving Biden’s potential Supreme Court nomination, big priorities and even routine business at risk in the face of Republican objections.

#### Voting Rights

Garcia 1-31-22

(George, former adviser to two governors of Puerto Rico Newsweek, lexis)

Even though Democrats knew that their voting rights bill was unlikely to pass, they spent an enormous amount of political capital on trying to move voting rights legislation in the Senate, with President Joe Biden visiting Georgia to champion the bill, and Senate Majority Leader Chuck Schumer pushed aggressively to carve out a filibuster exemption for the bill which was defeated by Senators Joe Manchin and Kyrsten Sinema.

#### Plan popular.

Lande & Vaheesan ’20 [Robert; Professor of Law @ University of Baltimore School of Law and Sandeep; Legal Director @ Open Markets Institute, JD @ Duke; “Preventing the Curse of Bigness Through Conglomerate Merger Legislation,” *Ariz. St. LJ* 52; AS]

B. Growing Political and Public Concern About Corporate Power

Public recognition of, and concern about, corporate political power is growing. An increasing number of politicians and public figures are focused on the political and social—as well as economic—power of large businesses. This concern is not limited to one portion of the political spectrum. A diverse set of voices and organizations are calling for tackling monopoly and oligopoly power in American society.

Prominent liberal and progressive voices have demanded action to curb the economic and political power of large corporations. Many Democrats have made strengthening anti-merger and anti-monopoly law a key pillar of their agenda.80 As mentioned in the introduction, Senator Amy Klobuchar introduced an anti-merger bill that would establish a presumption of illegality involving mergers that combined more than $5 billion in assets.81 This bill would target corporate size directly, although it features a large exemption for pure conglomerate mergers.82

Senator Bernie Sanders weighed in against the AT&T/Time Warner merger and identified the further agglomeration of power as a principal evil of the combination. 83 He stated this consolidation “represents a gross concentration of power that runs counter to the public good.”84 And in early October 2018, Sanders introduced a bill that would break up the largest financial institutions in the United States and establish a cap on size going forward.85 Senator Sanders also promised to combat the excesses of large firms in the agricultural sector, stating that they are devastating to the small farmer and are a direct cause of mass unemployment, lower wages, massive wealth inequality, and a host of social problems. 86 In his October 2019 Corporate Accountability and Democracy plan, presidential candidate Sanders condemned the present system in which “a small group of ultrawealthy CEOs are making the decisions that increasingly determine our economic, environmental and political future.”87

Senator Elizabeth Warren has offered extensive critiques of corporate power, citing undue political influence as one of the evils of corporate bigness.88 In a keynote address at a conference hosted by the Open Markets Institute in December 2017, Senator Warren warned that “[c]oncentrated market power also translates into concentrated political power—the kind of power that can capture our government. And that’s exactly what’s happening, as President Trump and the Republicans in Congress bow to the power and influence of these industrial giants and financial titans.”89 Warren promised that if elected president, she would break up Amazon, Facebook, and Google.90 She published a detailed plan to break up big tech companies, including the creation of a threshold of $25 billion in annual revenue, above which companies would be subject to restrictions and regulations including mandatory divestitures of certain portions of the company. 91 Facebook allegedly removed Warren’s political ads posted on Facebook that called for breaking up Facebook.92

Warren also called for breaking up some of the biggest farming corporations “so that they not only do not have that kind of economic power, so that they’re wiping out competition, so they’re taking all the profits for themselves . . . but also so that they don’t have that kind of political power.”93

These figures are not outliers but are representative of a growing antimonopoly philosophy among Democrats, liberals, and progressives. Others have echoed the concerns expressed by Senators Klobuchar, Sanders, and Warren. (Former) Representative (and current Minnesota Attorney General) Keith Ellison and sitting Representative Ro Khanna established an Antitrust Caucus and called for antitrust enforcers to look beyond just consumer welfare. 94 Alexandria Ocasio-Cortez, the Democratic representative for New York’s 14th Congressional district, has repeatedly voiced concerns about the political might of large financial institutions.95 Senator Cory Booker has lamented the “incredible concentration of economic and political power in this country” 96 and introduced a bill that would establish a moratorium on corporate mergers in agriculture. 97 Former Colorado governor and former presidential candidate John Hickenlooper has called for a major revival in antimonopoly enforcement.98

Indeed, many Democrats have criticized the political power of banks since at least the 2007–08 financial crisis. In early 2009, just six months after the collapse of Lehman Brothers and the start of the worst financial crisis in eighty years, Senator Richard Durbin famously observed that “the banks— hard to believe in a time when we’re facing a banking crisis that many of the banks created—are still the most powerful lobby on Capitol Hill. And they frankly own the place.”99

Among academics and commentators, Joseph Stiglitz and Paul Krugman have repeatedly sounded the alarm about the pervasive market power problem. Stiglitz has opined that “America has a monopoly problem—and it’s huge” and cited the political power of large corporations as subverting democracy. 100 Krugman has similarly recognized the corrosive political power of large corporations. 101 Former Secretary of Labor, Harvard professor, and political commentator Robert Reich applauded Elizabeth Warren’s announced intention to break up big tech and predicted that breaking them up would allow for more privacy, decentralization of information, and more innovation. 102 Barry Lynn, director of the Open Markets Institute think tank, has sounded the alarm that tech giants like Google and Facebook are a threat to core democratic institutions.103 Zephyr Teachout, a progressive law professor, promised that if elected Attorney General of New York she would explore breaking up Google and Facebook using New York state antitrust laws.104

Conservatives in the United States are generally supportive of, and deferential toward, big business interests. Conservative thinkers have indeed played a major role in weakening the antitrust laws and allowing consolidation and monopolization across the economy.105 In the name of “free markets,” conservative politicians and commentators typically favor policies that support large corporations and place few restrictions on them.106

Nonetheless, more and more conservative voices are starting to raise concerns about corporate power. At present, many of the attacks reflect anger at certain companies, more than corporate power in general. Much of the conservative criticism appears driven by the perceived politics of their executives and employees more than a distrust of large corporations and their power in general. For example, Google is viewed as supportive of the Democratic Party and some liberal causes and it has drawn significant criticism from the right. 107 Whatever the underlying motivation though, skepticism of large corporations, or at least a subset of them, is a growing strand of thought on the right.

At least on the surface, the Trump administration reflects this rising antimonopoly tendency among conservatives. President Trump has repeatedly attacked certain powerful corporations.108 He has criticized the power of Amazon and its founder and chief executive officer, Jeff Bezos. 109 He has also condemned vertical integration in telecommunications—specifically calling out the completed merger between Comcast and NBC Universal and the now-completed merger between AT&T and Time Warner—for threatening to “destroy democracy.”110 His former chief strategist and right-wing icon, Steve Bannon, called for public utility regulation of tech platforms like Facebook and Google.111 Former Attorney General Jeff Sessions called for remedying the perceived liberal bias of these same tech platforms.112

Others on the right have sounded similar fears about corporate power. Senator Ted Cruz, who has been a major recipient of campaign contributions from large corporations,113 has endorsed using the antitrust laws against the power of tech platforms. 114 Senator (and former Representative) Marsha Blackburn has criticized platforms like Google and YouTube for failing to practice viewpoint neutrality and called them out for apparent bias against individuals and organizations expressing conservative opinions. 115 Representative Jim Jordan (R-OH) expressed similar concerns and insinuated that stronger governmental measures should be applied to curb the power of giant social media companies.116 Senator Josh Hawley (R-MO) previously served as Missouri’s attorney general and, during his tenure, opened an antitrust investigation into Google.117

Some conservative media outlets have in recent years been vocal critics of corporate power. Breitbart, the hard-right news outlet formerly run by Steve Bannon, has championed antitrust enforcement against large corporations.118 The American Conservative, a nativist right outlet that supports economic populism, has become a consistent critic of corporate power and supporter of renewed antitrust enforcement.119 Tucker Carlson, a commentator on Fox News, has endorsed public checks on Facebook and Google.120

Conservative talk radio icon Rush Limbaugh described what he saw as a pernicious aspect to corporate ownership of media.121 He stated that large, non-media corporations or their CEOs, for example Jeff Bezos purchasing The Washington Post, acquire media to shape policy and thereby increase their power. 122 Even anti-government conspiracy theorist Alex Jones has called on the Trump administration to break up big technology companies because the supposedly left-leaning Silicon Valley titans are using their massive power to stifle conservative viewpoints.123

With rising awareness of, and opposition to, corporate power, an antimerger law that directly targeted corporate size could attract significant popular and political support. Senator Klobuchar’s bill has already introduced size-based limits on consolidation into the political debate.124 Many liberals and progressives appear ready to embrace this idea.125 On the right, support for such a possibility is much less certain.126 Yet, a growing tide of criticism from conservative figures suggests at least one faction on the right may be open to preventing corporate growth through extremely large mergers and acquisitions.127

#### Climate provisions have been gutted

Hawkins 1-21-22

(Howie, 2020 green party presidential candidate, Eurasia Review, lexis)

The only bipartisan "success" is a progressive nightmare. It is the passage of the military spending bill in which Congress gave the Pentagon $25 billion more than Biden asked for. Instead of emphasizing diplomacy and economic assistance to reduce conflicts around the world, the Biden administration with bipartisan support is saber-rattling, sanctioning, and escalating tensions with China, Russia, and a host of smaller countries that refuse to kowtow to U.S. dictates. Meanwhile, progressive domestic priorities have been killed. The Green New Deal is off the table. The ever-shrinking Build Back Better bill's far more limited climate program is on life-support at best. Instead of declaring a climate emergency and taking available executive actions for climate protection, Biden is permitting oil and gas drilling and pipelines at a faster rate than Donald Trump.

# 1AR

## States CP

### XT 2AC 5: Patent Preemption

#### Gets preempted.

Richard Samp 14. Chief Counsel, Washington Legal Foundation. JD from M\*chigan. “The Role of State Antitrust Law in the Aftermath of Actavis”. 15 Minn. J.L. Sci. & Tech. 149. Winter 2014. Lexis, accessed thru Dartmouth.

This paper concludes that state antitrust liability can be imposed on parties to patent settlements so long as the state action "parallels" federal antitrust law. On the other hand, state law is preempted to the extent that it seeks to impose antitrust liability for conduct not deemed actionable under federal law; under such circumstances, state-law liability would be impliedly preempted because it would stand as an obstacle to accomplishing the purposes of federal patent law. The scope of preemption likely would include any effort by states to apply a stricter standard of review to reverse payment patent settlements--either a "quick look" review accompanied by a presumption of illegality, or a declaration that such settlements are "per se" illegal.

Part I of this paper summarizes federal preemption law as it has been applied to state antitrust actions. It explains that the U.S. Supreme Court has never interpreted federal antitrust law as imposing a limit on states' authority to regulate business practices deemed by states to have anticompetitive effects. Nonetheless, federal courts have not hesitated to rule that state antitrust law is preempted by federal law when they determine that state law comes into conflict with some other federal statute. In this instance, the relevant "other federal statute" is federal patent law.

#### Interoperability falls out of scope of federal antitrust law – nascence.

Chinmayi Sharma 19. JD, UVA Law. “Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability”. 50 U. Mem. L. Rev. 441. Winter 2019. Lexis. Gendered language [corrected].

The Commission adjudicates cases involving competition harm and cases involving consumer protection, 178and API regulation can comfortably fit within each of the available enforcement avenues. First, restrictive APIs are especially pernicious examples of incipient anticompetitive behavior that often fall out of the reach of Sherman and [\*481] Clayton challenges due to their nascence. There is already precedence for Section 5 activity in this space with the cases brought against Silicon Graphics and Intel challenging their breaks in technological interoperability. 179Second, the FTC has already relied on novel consumer protection theories to bring privacy cases, arguing that insufficient data security violates accepted norms and consumer expectations. 180 Competition harm and consumer protection cases are distinguished based on the identity of the victim whether the challenged activity predominantly injures competitors or end-users. 181But the Agency and courts have acknowledged that the line between the two has blurred in modern cases, both because of a renewed legislative emphasis on consumer interests 182and the recognition that the impact on competitors can be transferred downstream to directly injure consumers. 183

#### Patent defenses are extensive and their existence deters market entry.

EFF 13. “Patents”. Electronic Frontier Foundation. Feb 28 2018. https://www.eff.org/deeplinks/2013/02/deep-dive-software-patents-and-rise-patent-trolls

Beloved podcasts like the Adam Carolla Show and HowStuffWorks are under attack. They and other podcasts are getting sued for, well, podcasting. And they're not the only victims—developers are being targeted for building mobile apps, and offices around the nation are being attacked for using ordinary networked scanners. These creators are only a few of the thousands of victims of one of the biggest threats to innovation: patent trolls.

Patent trolls are entities that don't create products themselves, but instead buy patents and make money from lawsuits. Trolls often make broad claims of infringement based on patents of questionable validity, and most defendants choose to settle because of the outrageous nature of patent litigation. It is risky and expensive—and trolls offer settlement amounts that, although incredibly burdensome, are cheaper than a lawsuit, which can often cost well into the millions of dollars.

This week, Congress made huge strides with the introduction of the SHIELD Act—a bill that, if passed, would become the first legislation to directly address the problem of patent trolls. The Saving High-Tech Innovators from Egregious Legal Disputes (SHIELD) Act, introduced by Reps. Peter DeFazio (D-OR) and Jason Chaffetz (R-UT) in the House, directly targets the trolls' incentive model. The bill creates a system where if a troll loses in court because the patent is found to be invalid or there is no infringement, then it pays the other side’s costs and legal fees.

This bill marks an important step toward ending the patent troll problem for good. We encourage you to tell your lawmakers to support the SHIELD Act. Read on and discover how patent trolls became such a problem.

The Flood of Software Patents

Software patents are relatively new phenomena; the software industry grew from nothing into a mature business without any need for patent protection. For decades, the Patent & Trademark Office (PTO) was generally reluctant to issue patents that covered software. But in the mid-1990s, the Federal Circuit (the court that hears patent appeals) first held that an algorithm implemented in a general-purpose computer could be patentable.

This opened the floodgates for software patents. The PTO now issues about 40,000 software patents a year. That's more than 100 per day. Unfortunately, the quality of these patents has tended to be very low. On average, examiners spend only 18 hours reviewing each patent application. This is not nearly enough time to properly check if the invention is new. To make things worse, the claims in software patents (this is the language that is supposed to mark the boundaries of the invention) are often vague and overbroad—giving unscrupulous patent owners the ability to claim that their patent covers a wide range of technology.

The Rise of The Patent Troll

The rise in such broad software patents created an environment ripe for patent trolling to surge in popularity. Since 2005, the number of patent troll lawsuits per year has skyrocketed—a four-fold increase to over 5,000 lawsuits every year. By 2012, for the first time ever, more than half of all patent suits were brought by trolls.

Patent trolls often sue with weak software patents, so when they are actually challenged in court, they usually lose. From 1995-2011, patent trolls won fewer than 25% of cases that went to judgment. And the most aggressive trolls fare even worse: of the most frequently litigated patents (those asserted in eight or more lawsuits), the trolls won fewer than 10% of their cases.

Unfortunately, patent litigation is so expensive that it is often cheaper to pay the troll to go away. Even for smaller companies, the average cost of defending a patent case all the way through trial approaches $2 million. Despite these costs, some companies—like Newegg and Twitter—have fought back and won. But the astronomical expense of patent litigation means that most defendants will settle.

With the explosion of patent troll lawsuits, most technology companies can expect to be targeted at some point. The patent troll motto seems to be: if you build anything, we will come. The result is that patents—especially the vague and overbroad software patents beloved by trolls—act as a disincentive to innovate and create.

Trolls Target Startups and End Users

In recent years, patent trolls have increasingly targeted smaller firms that are less likely to fight back. A recent study showed that more than half of the firms sued by patent trolls have less than $10 million in annual revenue—with startups being a common target.

Another disturbing trend is patent trolls going after end users for everyday tasks. For example, a patent troll has sued restaurants, hotels, and companies for using Wi-Fi. And another troll has blanketed the nation with letters demanding that companies pay $1,000 per employee for using standard office technology like scanners and email.

Software Patents Hurt Innovation

In the hands of patent trolls, software patents are a tax on innovation. And this tax is getting bigger every year. In 2011, companies made $29 billion in direct payouts to patent trolls. And the overall cost to the economy has been estimated at about $80 billion per year. Every dollar spent fighting or paying off a troll is a dollar not spent on launching new products and creating jobs.

#### It inhibits interoperating.

Cory Doctorow 21. Special consultant to the Electronic Frontier Foundation, MIT Media Lab Research Affiliate, visiting professor of computer science at the Open University, visiting professor of practice at the University of North Carolina’s School of Library and Information Science, co-founder of the Open Rights Group. “The Future is in Interoperability Not Big Tech: 2021 in Review”. EFF. Dec 24 2021. https://www.eff.org/deeplinks/2021/12/future-interoperability-not-big-tech-2021-review

But tech’s had network effects on its side since the earliest days, and yet the web was once a gloriously weird and dynamic place, where today’s giant would become tomorrow’s punchline - when was the last time you asked Jeeves anything, and did you post the results to your Friendster page?

Network effects aren’t anything new in tech. What is new are the legal strictures that prevent interoperability: new ways of applying cybersecurity law, copyright, patents, and other laws and regulations that make it illegal (or legally terrifying) to make new products that plug into existing ones.

That’s why you can’t leave Facebook and still talk to your Facebook friends. It’s why you can’t switch mobile platforms and take your apps with you. It’s why you can’t switch audiobook providers without losing your audiobooks, and why your local merchants don’t just give you a browser plugin that replaces Amazon’s “buy” buttons with information about which store near you has the item you’re looking for on its shelves.

These switching costs are wholly artificial. By their very nature, computers and networks are flexible enough to allow new services to piggyback on existing ones. That’s the secret history of all the tech we love today.

Interoperability - whether through legally mandated standards or guerilla reverse-engineering - is how we can deliver technological self-determination to internet users today. It’s how we can give users the power to leave the walled gardens where they are tormented by the indifference, incompetence, and malice of tech platforms, and relocate to smaller, more responsive alternatives that are operated by co-ops, nonprofits, startups, or hobbyists.

#### The DMCA – which is a *federal protection* – prohibits interoperating.

Cory Doctorow 19. Special consultant to the Electronic Frontier Foundation, MIT Media Lab Research Affiliate, visiting professor of computer science at the Open University, visiting professor of practice at the University of North Carolina’s School of Library and Information Science, co-founder of the Open Rights Group. “A Cycle of Renewal, Broken: How Big Tech and Big Media Abuse Copyright Law to Slay Competition”. EFF. Aug 19 2019. https://www.eff.org/deeplinks/2019/08/cycle-renewal-broken-how-big-tech-and-big-media-abuse-copyright-law-slay

It's easy to imagine that this is the general cycle of technology: a new technology comes along and rudely shoulders its way into the marketplace, pouring the old wine of the old guard into its shiny new bottles. The old guard insist that these brash newcomers are mere criminals, and demand justice.

The public flocks to the new technology, and, before you know it, the old guard and the newcomers are toasting one another at banquets and getting ready to sue the next vulgarian who has the temerity to enter their market and pour their old wine into even newer bottles.

That's how it used to work, but the cycle has been interrupted.

The Cycle is Broken

In 1998, Congress passed the Digital Millennium Copyright Act, whose Section 1201 bans bypassing a "technological measure" that “controls access” to copyrighted works. The statute does not make an exemption for people who need to bypass a copyright lock to do something legal, so traditional acts of "adversarial interoperability" (making a new thing that plugs into an old thing without asking for permission) can be headed off before they even get started. Once a company adds a digital lock to its products, it can scare away other companies that want to give it the broadcasters vs records/cable vs broadcasters/VCRs vs cable treatment. These challengers will have to overcome their fear that "trafficking” in a “circumvention device" could trigger DMCA 1201's civil damages or even criminal penalties—up to $500,000 and 5 years in prison...for a first offense.

When companies like Sony made the first analog TV recorders, they focused on what their customer wanted, not what the winners of last year's technological battle thought was proper. That's how we got VCRs that could record off the air or cable (so you could record any show, even major Hollywood movies getting their first broadcast airing) and that allowed recordings made on one VCR to be played on another recorder (so you could bring that movie over to a friend's house to watch with a bowl of popcorn).

Today's digital video products are different. Cable TV, satellite TV, DVDs/HD DVDs/Blu-Ray, and streaming services all use digital locks that scramble their videos. This allows them to threaten any would-be adversarial interoperators with legal reprisals under DMCA 1201, should they have the temerity to make a user-focused recorder for their products. That stifles a lot of common-sense ideas: for example, a recorder that works on all the programs your cable delivers (even pay-per-views and blockbusters); a recorder that lets you store the Christmas videos that Netflix and Amazon Prime take out of rotation at Christmastime so that you have to pay an upcharge to watch them when they're most relevant; or a recorder that lets you record a video and take it over to a friend's house or transfer it to an archival drive so you can be sure you can watch it ten years (or even ten minutes) from now.

Since the first record players, every generation of entertainment technology has been overtaken by a new generation—a generation that allowed new artists to find new audiences, a new generation that overturned the biases and preconceptions of the executives that controlled the industry and allowed for new modes of expression and new ideas.

Today, as markets concentrate—cable, telecoms, movie studios, and tech platforms—the competition is shifting from the short-lived drive to produce the best TV possible to a long-term strategy of figuring out how to use a few successful shows to sell bundles of mediocre ones.

In a world where the cycle that led to the rise of cable and streaming was still in effect, you could record your favorite shows before they were locked behind a rival's paywalls. You could search all the streaming services' catalogs from a single interface and figure out how to make your dollar go farther by automatically assembling a mix of one-off payments and subscriptions. You could stream the videos your home devices received to your phone while you were on the road...and more.

And just as last year's pirates — the broadcasters, the cable operators, the VCR makers — became this year's admirals, the companies that got their start by making new services that centered your satisfaction instead of the goodwill of the entrenched industries would someday grow to be tomorrow's Goliaths, facing a new army of Davids.

Fatalistic explanations for the unchecked rise of today's monopolized markets—things like network effects and first-mover advantage—are not the whole story. They are not unstoppable forces of nature. The cycle of concentration and renewal in media-tech shows us that, whatever role the forces of first-mover advantage and network effects are playing in market concentration, they are abetted by some badly written and oft-abused legal rules.

DMCA 1201 lets companies declare certain kinds of competition illegal: adversarial interoperability, one of the most historically tried-and-true methods for challenging dominant companies, can be made into a crime simply by designing products so that connecting to them requires you to bypass a copyright lock. Since DMCA 1201 bans this "circumvention," it also bans any competition that requires circumvention.

## Politics DA

### 1AR – AT: Warming Extinction

#### Extinction.

Deudney ‘18 [Daniel; Associate Professor of Political Science @ Johns Hopkins University; “Great Debate: The Nuclear-Political Question and World Order”; The Oxford Handbook of International Security]

The unexpected end of the Cold War is not the only major development over the nuclear era that was unanticipated. Most surprising are the underlying physical bases for nuclear weapons: a rare element—uranium—can be coaxed into releasing, pound per pound, a millions times more energy than chemical high explosives, and then the thermonuclear processes fueling the sun and stars could also be harnessed to produce explosions thousands of times larger than the one that obliterated Hiroshima. Also unexpected were the discoveries that a full-scale nuclear war would possibly render extinct all the higher life forms on the planet—including humans—by destroying the thin layer of ozone in the stratosphere blocking potent solar radiations, and that the (p. 341) soot from many burning cities could plunge the planet into a “nuclear winter” in which agricultural production would be severely curtailed for years (Schell 1981; Ehrlich et al. 1984). Although now taken for granted, it is surely surprising that the Soviet Union and the United States could deploy tens of thousands of nuclear weapons in a vast global- spanning network of bases and mobile platforms over several decades without a single weapon ever being detonated.

### XT 2AC 1: Wont Pass

#### BBB is dead

NBC News 2-3-22 https://www.nbcnews.com/politics/congress/manchin-says-build-back-better-dead-here-s-what-he-n1288492

Manchin once again said this week that the Build Back Better Act is “dead,” referring to the $2 trillion-plus bill that passed the House. A nonnegotiable red line for him is that all new programs must be permanent and fully financed.

#### Budget thumps every link

Independent View 1-31-22 lexis

A Shutdown is unlikely, but Members of the Senate Appropriations Committee from both Parties, Warn that if Negotiators blow through the Mid-February Deadline, it increases the likelihood that Biden will have to settle for a Yearlong Stopgap Funding Measure to keep the Government Open. That would Prevent him from putting his own stamp on Department and Agency Budgets while Democrats Control Congress. As a result, Senate Democrats, right now are Prioritizing passage of the Omnibus Spending Bill ahead of the Build Back Better (BBB) Act, which the House Passed in November, 2021, but then stalled last month because of Opposition from Sen. Joe Manchin (D-WV). 'I think the budget has to be next, to be honest. I want BBB to be done, but we have a narrow window to pass a budget, and I want to make sure we get a budget deal,' said Sen. Chris Murphy (D-CT), the Chairman of the Senate Appropriations Homeland Security Subcommittee, referring to the Omnibus Package. 'You have a limited window on a budget, and you never know what's going to happen in 2022. If we don't get a budget now, there's a chance President Biden will never do a budget with the Democratic Congress,' Murphy warned. 'If we miss this deadline, it becomes really hard to avoid a yearlong CR [Continuing Resolution],' he said.

#### That kills any chance of passage

Lillis 2-3-22

(Mike, https://thehill.com/homenews/house/592594-house-democrats-warn-delay-will-sink-agenda)

House Democrats of all stripes are pressing for quick action on the climate, health and education package at the heart of President Biden’s domestic agenda, warning that a long delay in revisiting the Build Back Better Act is the surest way to kill it. The lawmakers are citing a host of reasons for their pleas of urgency, including the fast-approaching midterm elections, the desperate desire to give an unpopular president a big boost and the party’s fragile Senate majority that’s just one tragedy away from flipping to GOP control — a dynamic highlighted this week when Sen. Ben Ray Luján (D-N.M.) announced that he’s recovering from a stroke. But the common theme is clear: Time, they say, is not on their side. ADVERTISEMENT “There are great dangers involved in dragging it out, including all kinds of intersecting battles,” said Rep. David Price (D-N.C.), a member of the House Appropriations Committee.

### XT 2AC 3-5: Thumpers

#### Lujan loss imperils entire agenda

AP 2-3-22 https://apnews.com/article/stephen-breyer-coronavirus-pandemic-joe-biden-us-supreme-court-health-618b25ed7ac76d07fa3a2a1c37b6f161

The uncertainty shows just how precarious the Democrats’ hold on power in Washington really is and the limits of Biden’s ability to usher what’s left of a once-bold agenda through Congress. The president’s chance to confirm a Supreme Court nominee, a hoped-for reset for the administration and the party, could be dangerously at risk if Democrats are unable to count on their majority to overcome hardening Republican opposition. Already, routine Senate business was being rearranged Wednesday, as the Senate Commerce Committee announced it would be postponing consideration of some of Biden’s executive branch nominees because the panel, on which Luján is a member, needs all Democrats for the votes. More pressing, though, is the upcoming Supreme Court confirmation battle to replace retiring Justice Stephen Breyer. Democrats have been eager to shift to the high court fight, believing it will galvanize voters at a time when Biden’s broader legislative agenda, including his sweeping Build Back Better Act and voting legislation, have collapsed. Sen. Dick Durbin, D-Ill., the chairman of the Judiciary Committee, said the panel is planning to push ahead with consideration of Biden’s Supreme Court pick as soon as the president announces his nominee, expected later this month. ADVERTISEMENT “We don’t anticipate any difficulties,” Durbin told reporters at the Capitol. Schumer has signaled a swift confirmation of Biden’s Supreme Court nominee. And after meeting with Biden at the White House, the majority leader’s spokesman said Luján’s absence is not expected to affect the Senate’s timeline for the process. The Senate is split 50-50, with Democrats holding an ever-so-fragile majority because Vice President Kamala Harris can cast a tie-breaking vote. As it stands, Biden’s agenda has fallen apart on Capitol Hill, taken down by the one-two punch of Republican opposition and two Democrats, Sens. Joe Manchin of West Virginia and Kyrsten Sinema of Arizona, who have joined Republicans to halt the president’s priorities. Luján’s illness is a reminder it’s not just Manchin, Sinema and Republican opposition, but the health and welfare of every single senator that could make or break the Democrats’ hold on power and the outcome of Biden’s agenda.

### XT 2AC 6: FTC Shields

#### Even if, FTC actions fly under the radar.

Baker ’19 [Jonathan; Research Professor of Law @ American University Washington College of Law, Frmr Chief Economist of the FCC & Director of Bureau of Economics FTC; *The Antitrust Paradigm*,p. 62-64]

Politics in this sense is largely foreign to the courts, including in the interpretation of antitrust statutes.51 At the federal antitrust enforcement agencies, politics almost never matters directly in case selection and evaluation,52 though it occasionally influences the choice of industries or conduct to investigate. 53 With rare exceptions mainly involving the Johnson and Nixon administrations, U.S. antitrust enforcement since the mid-twentieth century has been almost entirely insulated from direct political influence.54 The enforcement agencies occasionally testify before members of Congress or brief their staffs on completed matters and topical issues, but these are largely benign means of assuring agency accountability.55 There also is little reason to credit “revolving door” concerns—the suggestion that senior antitrust officials take positions to benefit their former private sector employers or clients or to enhance their future employment prospects.56

The judgment that modern U.S. antitrust enforcement has been largely free from direct political influence is not inconsistent with anecdotal evidence of corporate lobbying on antitrust matters. 57 In most recent examples, the primary target is Congress or sector regulators such as the Federal Communications Commission (FCC),58 not antitrust enforcement agencies or the courts. Occasionally, firms do undertake a substantial and expensive lobbying effort aimed solely at influencing the Justice Department or the Federal Trade Commission (FTC).59 It may be rational for businesses to do so even though political pressure is unlikely to affect enforcement outcomes. So long as the firm’s lawyers do not think that the lobbying will be counterproductive, and the costs of lobbying are small relative to potential benefits of avoiding enforcement, the businesses may be willing to invest in a long-shot effort to persuade. For similar reasons, the relevant firm’s opponents may undertake counter-lobbying. 60 It is important to keep in mind that the occurrence of lobbying does not imply its effectiveness. Firms may lobby other government agencies successfully, which might lead executives to suspect incorrectly that antitrust lobbying efforts will pay off too.

Relatedly, we need not be concerned that the stock market responds positively when firms announcing potentially questionable mergers also increase lobbying expenditures.61 That firms lobby harder when attempting to merge does not show that antitrust lobbying affects enforcement outcomes. At most it suggests that investors think this. Alternatively, and perhaps more likely, investors may view lobbying expenditures as a signal that a firm has also invested substantially in antitrust counseling, and thus that the firm has reasons to think that the transaction will survive antitrust review based on information known to it but unavailable publicly.

Based on my own experience, and the experience of colleagues who have served in senior federal enforcement agency positions, antitrust enforcement decisions at the Justice Department and FTC are invariably based on legal and policy arguments, the strength of the evidence, and institutional factors such as resource constraints—not on the identity of the interest groups or politicians favoring various outcomes. Political interest has led the agencies to open investigations, but it does not affect the resolution of individual law enforcement matters.