# open source texas 1

# 1ac – bc – texas

## 1ac – interoperability

### platforms advantage – 1ac

#### Advantage one is *platforms*.

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

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].

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 reduces network effects and switching costs of platforms – it allows users to leave platforms without losing ability to interact with them. That creates platform competition.

Becky Chao and Ross Schulman 20. Fellow at New America’s Open Technology Institute, former Millennial Public Policy Fellow at OTI, former honors paralegal at the Federal Trade Commission Bureau of Competition, BA in Public Policy from Duke. Senior counsel and senior policy technologist at New America’s Open Technology Institute, JD magna cum laude from American University, BS in computer science from Brandeis University. “Promoting Platform Interoperability”. New America. May 13 2020. 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

#### Platform competition prevents Internet balkanization. Monopolies create choke points that governments can target to shut down cross-border data flows.

Mark Lemley 21. William H. Neukom Professor, Stanford Law School. “THE SPLINTERNET”. 70 Duke L.J. 1397. March 2021. Lexis.

III. THE INTERNET IS WORTH SAVING

The result, I think, is that we're losing the internet. We're replacing it with "the splinternet," a balkanized set of computer [\*1419] protocols that increasingly differs by company and by country. That's not a good thing.

Now, you might not like some aspects of the internet. Some aspects of the internet are pretty horrible. Different countries may disagree about what's wrong with it. They may want to regulate it in different ways; they may want it to do different things. 111 But the internet has improved the world in all kinds of ways. Some of those are economic. The internet access industry alone generates a trillion dollars a year, 112 and that doesn't account for the commerce the internet makes possible.

The internet has also changed our lives for the better. Our phones improve our lives in ways we don't think about because we're not lost in a foreign country where we don't speak the language. We have a map that will get us where we want to go. We're not stuck on the highway with a flat tire and no way to communicate to anyone about that fact. We're not sitting in a restaurant waiting for a friend who canceled or debating some arcane fact with our friends without a device in our pocket capable of accessing all of the world's information.

For most of my lifetime, you did not take those things for granted. These are things that became available because we have access to this intersecting universe of information. Many of those benefits involve connection. They depend on the ability of systems to work together across multiple countries, across multiple languages. That's why the internet, and not a walled garden like Prodigy or CompuServe, is the thing we use today.

Balkanization means it's harder for people to share experiences across countries. Paul Ohm and Jack Goldsmith have argued that's a good thing, because we want different countries to have different rules, and those countries should be able to regulate the internet, just as they should be able to regulate any other part of their world. 113But I think we lose something real when we splinter the internet. Doing so takes away the ability to see what the rest of the world has, how the rest of [\*1420] the world thinks, and that's a loss. I think it's a loss for everyone, but it's a particular loss for people in repressive regimes who can look to the outside world for hope, for inspiration to demand change, and for the means of facilitating that change. If we take that away by allowing repressive governments to control how their citizens see the internet, we take away the prospect of freedom for a substantial number of people.

The internet famously enabled democratic uprisings in the Arab Spring. 114But splintering the internet also means it's easier for repressive governments to shut down outside access altogether--as Belarus, 115Iran, and Turkey have done recently, and as India has done in Kashmir during its crackdown on minority groups. And even if they don't shut down the internet altogether, those countries will end up with much more significant control over the companies who are providing the information to you if those companies are local. 116

The global nature of internet companies has mitigated that risk to some extent. If China wants to censor Google, Google can tell China to pound sand, and it did. 117Medium can tell Malaysia to pound sand, and it did when it was told to censor content that Malaysia didn't like. 118Baidu can't do the same with China because Baidu is in China. And an Iranian-based internet company or a Russian version of Wikipedia shouldn't be expected to offer much resistance to the demands of the nations where they are based. 119

[\*1421] Nationalized surveillance-enabled systems aren't just enabling government repression. They're also a cyber-security nightmare. Collect all of the sensitive data about what people are saying, what they're doing, what their accounts look like in a government system, and that government system will be hacked. I guarantee it. The more valuable the data the government collects, the bigger the target its database will be. And we've built not just our political and our social polity and conversation into the internet, we've built many of our most important systems around the internet backbone. Your banks, your power companies, various things that we depend on for the infrastructure of modern civilization are built into a network that we are increasingly making a nationalized, hackable, surveilled system. And the idea that governments--U.S. or foreign--will have more control over them is troubling.

The worst thing to me about the splintering of the internet is that I think the way we're losing the internet parallels the way we're losing the project of globalization. Globalization sometimes gets a bad rap, 120but for me, it is something valuable. And we are replacing globalization with a particularly authoritarian form of tribalism in countries around the world: in the United States, the United Kingdom, China, Russia, India, Brazil, Turkey, Hungary, and the Philippines. 121In country after country, the future seems to lie not in reaching out and interacting with the world around you, but in autarkies. Countries are drawing boundaries around their race, their nationality, their religion, and so forth. The splintering of the internet reflects that retreat from globalization, but it may also make it harder to undo. One possible mechanism for unifying the internet--international law and international norms--seems less promising than it would be in a world that was more committed to cooperation. And the results may be catastrophic. 122

[\*1422] IV. WHAT CAN WE DO?

That brings me to the last part of the speech, the part where I tell you how to solve the problem. Unfortunately, I don't have great ideas. Nonetheless, here are four suggestions.

First, we should promote technologies that are resilient to government censorship. End-to-end encryption of phones and messaging is a good start. We ought to be building it into all of our systems, and we ought to be using systems only if they are, in fact, encrypted. Encryption and blockchain-based technologies can allow persistent pseudonymity, so that people can actually interact with a verifiable person without having to identify them and know who they are. 123VPNs--or "Virtual Private Networks"--can allow tunneling through national firewalls to give you access to other people's internet experiences. 124We need to protect and promote these technologies, not undermine them. People can use them to avoid censorship in countries that engage in software filtering. 125That means we need to fight government efforts to introduce back doors wherever we can, not just when China imposes them, but when the United States tries to impose them on Apple phones as well.

Right now, many of these technologies are fringe. If you use blockchain--or peer-to-peer networks, back in the day--the assumption is that there's probably something wrong with you. Maybe you're a drug dealer or you're engaged in copyright piracy or something. We often associate these fringe technologies with criminals, simply because we haven't developed a mainstream tradition of using them. And without widespread legitimate use, much of the early use of these technologies is indeed by criminals. 126

But that conclusion isn't inevitable. The same thing was once said of secured-sockets-layer ("SSL") encryption. Indeed, the United States tried to block encryption from being built into the internet back [\*1423] in 1995. 127Now it's standard. You wouldn't want to give your credit card number to somebody, much less bank with them, if they didn't actually have a secure transaction with robust encryption. What was once considered a dangerous fringe technology that was going to allow criminals to get away with all sorts of stuff is now something so standard that we get nervous if a website doesn't have it. The same could turn out to be true of end-to-end encryption or blockchain if mainstream sites adopt them widely enough.

Widespread adoption of these technologies of connection makes balkanization harder. And at a minimum, countries that hope to protect the internet shouldn't be making them illegal, either directly or through regulation via indirect devices like copyright anticircumvention. 128The law should resist the inference that you're facilitating a bad act by being anonymous or encrypted, and so we need to stop you. Unfortunately, the U.S. government often takes that position, and it has restricted the deployment of freedom-enhancing technologies like end-to-end encryption. 129

Second, individuals ought to resist hyper-personalization in the private market. We ought to be troubled by device and software specialization by private companies for some of the same reasons we resist balkanization by countries. Google, Tencent, Apple, and others want to keep you in their ecosystem. 130 They want to send you from their search engine to their pet systems, their apps, and their devices, because the longer they can keep you in the ecosystem, the more information they can learn about you and the more opportunities they have to sell you things. So they are closing Applications Programming Interfaces ("APIs") and making it harder for independent companies to write software that works with their ecosystems. 131

[\*1424] Venture outside. Don't use software only from your country. Don't use software all from the same company. Resisting the walled gardens at the private level helps preserve the internet and prevents it from devolving back into AOL or Compuserve.

Third, the law should promote interoperability across walled gardens. One way to do this is to encourage open APIs both as a business and a legal matter. Another way is open-source or free software. The law shouldn't mandate free software, but it should allow what Cory Doctorow calls "adversarial interoperability." 132

Companies want to create walled gardens. They want to regulate who can see in over the wall, who can get access to that information. The law has not traditionally let them, 133but a number of legal tools, including the Computer Fraud and Abuse Act and copyright law, have been used increasingly to try to prevent interoperability. 134Those laws threaten to prevent competitors from making a software program that, [\*1425] say, allows Facebook users to share their data across Facebook and other platforms. That preserves incumbents by making it harder to build an alternative to Facebook. That is especially true in markets with significant network effects. 135

Now, there are arguably good reasons why you want to prevent some sharing of data from incumbent platforms. One justification is privacy--people don't necessarily want the data they share with Facebook passed on to other companies without Facebook's consent. 136Although I have to say that the idea that Facebook is out there protecting your privacy by preventing you from using a cross-platform app--which they successfully did in Facebook, Inc. v. Power Ventures, Inc. 137--is a bit far-fetched to me.

But lack of open interfaces means concentration of private economic power. It means we all end up having to choose a single system. And in a market with strong network effects, that generally means all or most of us use the same system. And that, in turn, creates a central choke point governments can target.

That leads me to my fourth recommendation, which is we ought to be looking for mechanisms to promote vibrant competition in internet platforms. As Andrew McCreary and I explain in our paper, "Exit Strategy," 138 we no longer see the sort of Schumpeterian competition that has driven the tech industry for the last several years, in which one company comes out of nowhere and displaces the dominant market company. That used to be a central feature of technology markets, but it hasn't happened for a long time. If you look at the dominant companies--Google, Facebook, Apple, Amazon, Netflix--none of them are less than fifteen years old. 139Most of them [\*1426] are more than twenty years old. That's a long time to be dominant in the notoriously fast-moving tech industry.

We argue in Exit Strategy that we can trace this stalled competition to the venture-capital model we used to fund the tech industry. Venture capitalists fund companies with the intention of cashing out sooner rather than later. While thirty years ago that cash out generally involved an IPO that kept the startup in the market, today most startup exits involve selling the company. And increasingly those sales are to dominant incumbents. We are encouraging founders not to build their company into the new Google killer, but to sell out and to sell out to the incumbents--to Google itself. 140 We argue that we need more robust antitrust law restricting mergers. We also need to rethink the way we fund startups and reorient them toward competition rather than selling out to incumbents. 141

But whatever the reason we have lost it, we need competition in platforms. Competition is a good thing in itself. It produces better and cheaper services. But ironically, a more fragmented market may produce a more robust internet. Without competition--without choice--it becomes much easier to think of your internet provider as your regulator, insisting that the government compel them to control speech on their platform. Bigger, older companies may be more likely to comply with even unlawful or unreasonable government requests; they have more to lose by resisting the government. And it is easier for governments to regulate a single, central platform than decentralized technologies.

#### Internet fracturing hinders transnational intel collection – key to respond to gray zone conflict.

Erol Yayboke et. al 21. Director and Senior Fellow, Project on Fragility and Mobility, M.P.A. from the Lyndon B. Johnson School of Public Affairs at UT Austin. Carolina Ramos, research associate, International Security Program, MA candidate at Georgetown SFS. Lindsey Sheppard, Adjunct Professor at GW. “The Real National Security Concerns over Data Localization”. CSIS. Jul 23 2021. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization

How Data Localization Concerns National Security

Data localization puts at risk the global interconnectedness that has been the foundation of post–World War II peace and alliances and has been associated with a related overall decline in internet freedom. It has been used to target minority communities, activists, and journalists, often under the false pretense of protecting them. The resilience of democratic actors to authoritarian targeting is crucial; without it, countries that are increasing controls on their citizens, expanding their reach abroad, and exporting the tools and tactics of digital authoritarianism today could become the U.S. national security concerns of tomorrow.

The real national security concerns over data localization are often overshadowed by both manipulative interpretations of “national security” in support of more localization (as discussed below) and by economic and commercial arguments against it. These latter arguments abound, especially from those who believe that a free, open, secure, and reliable internet is a critical component of global trade and prosperity. Though many of the individuals and organizations making such arguments are in the United States, the pre-Brexit UK government warned in 2017 that such “Balkanization of the internet risks stifling the competition, innovation and trade which produce better services for consumers, and can weaken data security.” Regarding the information and communications technology (ICT) sector, evidence suggests that data localization increases prices and “[limits the] availability of ICT products and services while creating few data center jobs.” Despite economic protectionist arguments that cross-border data flows could make local internet-based businesses less competitive, there is limited evidence to suggest that data localization drives local economic development, online or off. Efforts to erect barriers might provide short-term commercial benefits to newly advantaged domestic firms, though potentially at the expense of innovation and the broader, long-lasting global economic growth spurred by the advent of the internet.

Despite these economic arguments against, the dominant global trend is toward more localization of data, leaving private-sector tech firms with difficult choices. Some multinational corporations have chosen to leave certain markets rather than comply with restrictive data localization mandates, while others have chosen to remain and adapt. Driving this trend are, in large part, governments making decisions based on their own interpretations of “national security.”

THE NATIONAL SECURITY CASE FOR LOCALIZING DATA

There is a case to be made that the free flow of data to hostile or authoritarian regimes threatens the national security of their geopolitical adversaries. For example, South Korea does not want data on its citizens and corporations to be accessible by North Korea. India and the United States have valid concerns about Chinese-owned companies—and, by extension, the Chinese Communist Party (CCP)—having access to their citizens’ data. Further, there are legitimate reasons why law enforcement agencies, for example, would desire both access to data and to restrict the ability of malign actors to share data across international borders. While a communiqué by G20 finance ministers ahead of the aforementioned Osaka Leaders’ Declaration mentions the benefits and challenges of data flows, the challenges are not clearly defined, and the language clearly attempts to give G20 member countries—which represent more than 80 percent of the world’s GDP and 60 percent of its population—leeway to impose data localization requirements as they see fit.

For G20 member countries such as China, India, Indonesia, Russia, and Turkey, the lack of an agreed-upon definition of data localization-related national security concerns provides an opportunity to argue for stronger data localization mandates. Some of these justifications lack evidence; others strain credulity. The government must control data, the argument goes, to protect its citizens’ privacy from external actors, despite there being no guarantee that data localization protects personal privacy any more than current cross-border flows do. In fact, data localization may undermine privacy by placing user data firmly within reach of governments or because of the deleterious effects data localization requirements have on cybersecurity. Beyond privacy, the most common excuse used to promote data localization is a nebulous and broadly defined version of “national security,” even though control over data flows has enabled governments to assert control over citizens more than it has addressed legitimate cybersecurity and other traditional national security concerns. In other words, control over data flows is often not actually about national security; it is about control.

The lack of an agreed-upon definition of data localization-related national security concerns provides an opportunity to argue for stronger data localization mandates.

THE NATIONAL SECURITY CASE AGAINST LOCALIZING DATA

Data localization—and the resulting fracturing of the internet—does have national security implications. These can be placed into three broad categories, which collectively constitute arguments against localizing data: (1) authoritarian threats to democracy, (2) limits on security actors’ collaboration and capabilities, and (3) cybersecurity threats.

1. Data localization can be used as a tool of digital authoritarianism to limit democracy and human rights. A recent CSIS policy brief defined digital authoritarianism as “the use of the internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties.” The brief also points out that “human rights and civil liberties are at risk, including freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy, online and off. Digital authoritarianism co-opts and corrupts the foundational principles of democratic and open societies; its goal is not just to break them down, but to redefine and reshape them in their authoritarian image.”

Data localization territorializes data so that domestic governments can assert jurisdiction over it and, by extension, service providers. This is intended to facilitate these governments’ ability to carry out a “crackdown on free expression, privacy, and a range of human rights,” especially in jurisdictions with authoritarian governments or weak democracies. Often, these data localization mandates are put forth under the guise of “protecting” individuals’ privacy or security, but the result is often the exact opposite. When citizen data—from Google Maps searches to Instagram likes to TikTok posts—is forced to be stored on local servers, governments have greater opportunities to use these data to gain greater control over the population. From Bangladesh to China to Russia and beyond, this manipulation enhances and strengthens the modern digital surveillance and censorship state.

It might make intuitive sense for a country to want to control “critical,” “highly sensitive,” or (as the Chinese government calls it) “important” data lest it fall into the hands of nefarious overseas actors. However, when the definitions of these terms are broadened and made more subjective over time, this increasing control has potentially negative effects on civil society, democracy, and human rights.

2. Data localization can limit collaboration between military, law enforcement, intelligence, and other security actors by creating obstacles to accessing information across borders. It effectively provides a safe haven for actors who execute gray zone tactics, including information operations via social media and illicit financial activities, on platforms subject to localization requirements—limiting the ability of targeted countries to combat and investigate them and, if applicable, prosecute the perpetrators of related crimes.

Cross-border law enforcement cooperation is often governed through the mutual legal assistance treaty (MLAT) system, though many MLATs “were drafted prior to the Internet’s widespread global adoption and therefore few of the treaties address core questions of data and jurisdiction” and “frequently do not specify what constitutes ‘protected data.’” In practice, this means that even as requests for data through the MLAT system increase (one 2015 estimate by the U.S. Department of Justice indicated a 60 percent increase in “requests for assistance from foreign authorities” over the previous decade), the system cannot handle sharing the data necessary for today’s law enforcement needs. If U.S. friends and allies adopt stricter data localization requirements, it could further complicate an already convoluted and outdated MLAT system, increasing barriers to law enforcement in the growing number of cases involving data that flowed across international borders. This would weaken current information-sharing channels and businesses’ reporting obligations, thereby impacting intelligence-gathering methods and criminal investigations. These methods are deployed daily, whether in response to a natural disaster or a cyberattack on a critical supply chain.

Additionally, Americans abroad, including U.S. government officials, depend on secure telecommunications that become more complicated as data localization requirements harden. The accuracy and credibility of data funneled through local systems are necessarily questioned, especially in countries with adversarial relationships with the United States. It can also further culturally isolate nations from one another, making diplomacy and peacebuilding efforts more difficult. Most specifically, if certain forms of data localization (such as hard or hybrid) are widely adopted, they could impede research into terrorist organizations’ funding structures, compromise informants, and weaken traditional U.S. intelligence-gathering networks.

#### Gray zone tactics break down strategic stability – ensure *wormhole*-style nuclear escalation.

Rebecca Hersman 20. Senior Adviser, International Security Program, and Director, Project on Nuclear Issues, Center for Strategic and International Studies, former deputy assistant secretary of defense for countering weapons of mass destruction at the DOD, former senior research fellow with the Center for the Study of Weapons of Mass Destruction at the National Defense University. “Wormhole Escalation in the New Nuclear Age”. Texas National Security Review. Summer 2020. https://tnsr.org/2020/07/wormhole-escalation-in-the-new-nuclear-age/

On Oct. 24, 1962, the United States raised its alert levels to defense readiness condition (DEFCON) 2, for the first — and thus far only — time in its history. In a televised address, President John F. Kennedy made clear that any nuclear attack from Cuba would be construed as an act of war, and that the United States would retaliate in kind. Had these events taken place today, the signaling almost certainly wouldn’t have stopped — or started — there. A chorus of pre-established online trolls messaging a Soviet-orchestrated storyline and all-caps Twitter threats would likely have come next. A targeted campaign to weaponize social media, turn elements of the American public against the president, and undermine the institutional authority and credibility of America’s deterrent did not arise because the technology to do so in real time did not exist. Instead, Kennedy stood “eyeball to eyeball” with Soviet First Secretary Nikita Khrushchev during the 13-day standoff until cooler heads prevailed. Flash forward and today’s global pandemic crisis offers a glimpse into how a toxic mix of disinformation, conspiracy theories, and digital technology can complicate effective crisis management, fuel competition and rivalry, shift blame, and sow mistrust.

Unlike traditional concepts of escalation, which suggest linear and somewhat predictable patterns from low-level crisis to all-out nuclear war,1 escalatory pathways in this new era of strategic competition will be less predictable. Indeed, increasingly sophisticated sub-conventional tactics such as disinformation and weaponized social media, the blurring of nuclear-conventional firebreaks, and the continuing diffusion of global power to regional nuclear states are adding new challenges and additional complexity to crisis management even as an increasingly competitive and contested security environment fuels greater coercive risk-taking among nuclear-armed states, in particular, the United States, Russia, and China.

The increasing use of hybrid warfare and gray-zone tactics by China and Russia reflects the view that their strategic aims are best achieved through coercive means below the level of direct conventional military interaction. Of course, these countries are not strangers to information warfare, propaganda, and deception, or even using proxy and covert warfare as tools of strategic competition (nor is the United States). Cold War history is littered with such cases from election manipulation to state-sponored rebel insurgencies. Moreover, from the Color Revolutions to Stuxnet, U.S. government actions, both real and imagined, have fed perceptions of a United States bent on shrinking Russia’s and China’s spheres of influence and shaping regional balances of power on favorable terms. And yet, in the aftermath of the Soviet Union’s collapse, America’s conventional military primacy, its ability to utilize the institutions and alliances of the liberal international order to advance U.S. interests, and its domestic political commitments to a free press and open internet have limited both the need and ability of the United States to compete aggressively in the gray zone.2 Both Russia and China, on the other hand, have felt compelled to challenge institutional structures and avoid direct traditional military competition, while pursuing asymmetric approaches to competition “below and beyond” traditional one-upmanship in the conventional military domain. Through broad, sub-conventional influence campaigns and the engagement of digital proxies, these states hope to advance their interests without clear attribution or risk of escalation.

These strategies of strategic competition in the sub-conventional domain may not be entirely new, but the tools that enable them have transformed the strategic significance of the unconventional battlespace and the coercive power of hybrid warfare. Fueled by technological innovation — particularly in digital media-based technology as well as cyber operations, artificial intelligence (AI), and machine learning — today’s competitive landscape is more complex and dynamic than before. The growing number of weapons in the sub-conventional arsenal include a range of kinetic and non-kinetic coercive tools, tactics, and strategies. The rise of the cyber domain; connectivity of global commerce, finance, and communications; speed and penetration of the internet; and prevalence and intimacy of social media that reaches nearly 40 percent of the world’s population have reshaped the competitive domain now commonly called the “gray zone”.3 Today’s proxies and surrogates look more like online trolls who wander freely inside one’s digital homeland, enabled by advanced cyber and disinformation tools and weaponized social media, rather than armed guerillas fighting internal wars with black-market weaponry in distant territories. Moreover, these new forms of influence and information warfare are not the exclusive domain of great powers. Rather, the accessibility of information technology suggests a leveling of the playing field for great powers, non-state actors, states, and non-government entities alike.

This technological transformation is not limited to the sub-conventional domain. Advanced technology is also blurring the threshold between conventional and strategic conflict, including the increasing commingling of nuclear and conventional payloads on non-ballistic missile delivery systems such as hypersonic vehicles, long-range cruise missiles, or extended-range torpedoes, as well as ever more effective missile defenses. Similarly, conventional and strategic warning and surveillance assets and advanced command-and-control capabilities continue to be integrated in ways that potentially undermine escalatory firebreaks by creating new counterforce or precision strategic-strike opportunities and enhancing the potential efficacy of missile defenses. These developments may bolster incentives to move first and fast in a high-end conventional fight. As traditional firebreaks between conventional and nuclear warning and delivery systems erode and the strategic effects of cyber and space operations multiply, the ability to manage and maintain strategic stability grows more difficult.

Moreover, today’s major powers do not have the playing field to themselves. The bipolarity that characterized strategic competition during the Cold War has disappeared and the U.S.-dominated unipolarity that characterized the immediate aftermath of the Soviet Union’s collapse has largely dissipated. Instead, today’s security environment is characterized by complex asymmetries, multi-domain conflict, and nine nuclear-armed states with widely divergent capabilities and intentions. Indeed, the rise of smaller nuclear powers has widened the nuclear shadow and its regional implications, particularly in areas where asymmetries in conventional capabilities and interests may create divergent beliefs about the utility of nuclear weapons in crisis bargaining scenarios.4 In parallel, states can now draw upon a growing range of strategic options, including long-range nuclear weapons; advanced conventional munitions; and space, cyber, and information capabilities. In this more fragmented competitive environment, emerging technologies, especially in the digital information space, can level the playing field, providing smaller states virtual expeditionary forces with global reach.

Of course, sub-conventional tactics, including information warfare and the use of surrogates, figured prominently throughout the Cold War and the many crises and close calls that characterized the period. During this time, while full-scale war between the United States and the Soviet Union was averted, lower-level conflict was widespread. In 1965, Glenn Snyder first proposed the existence of a “stability-instability paradox” to explain why mutually deterred, nuclear-armed adversaries sometimes engage in extensive, seemingly unstable, conflict and competition even while preserving comparative stability at the strategic level.5 As Robert Jervis later described it, “To the extent that the military balance is stable at the level of all-out nuclear war, it will become less stable at lower levels of violence.”6 In other words, strategic stability at the nuclear level could actually encourage or enable conflict at lower levels of the spectrum, especially through the use of surrogates or proxies. Seemingly, this allowed great powers not only to keep small wars and big wars separate, but also to engage in levels of sub-strategic conflict and competition even as the risks of nuclear war appeared to abate. Several behavioral rules seemed to help limit escalatory risks associated with this type of conflict, including not attacking the central territory of the adversary state, operating via surrogates and third parties where possible, and encouraging strategic transparency and crisis communications, especially following the Cuban Missile Crisis.

It is unclear if these same rules for strategic stability apply in today’s environment. Gray-zone competitions can now be deeply intrusive: Using witting and unwitting proxies within enemy territory, these tactics can strike at the heart of a country’s institutions, values, and populations well inside its digital homeland. Moreover, in this more fragmented, competitive landscape, the stabilizing of benefits of transparency and an assured second strike are unclear for countries with smaller arsenals and limited strategic geographic depth. Finally, while states continue to make use of proxies and surrogates, these digital soldiers may be both more intrusive and less controllable than those of the Cold War. This suggests the potential for a new nuclear paradox: As states drive to compete and win at the sub-conventional level — in the gray zone — the risk of strategic crisis may increase, even as the risk of conventional conflict between nuclear-armed states declines.

This new era of strategic competition will require renewed thinking about the tools and concepts of deterrence and escalation — adapting older ideas and developing new ones. Herman Kahn’s 44-rung “escalation ladder,” which describes a continuous, linear escalation path between low-level crisis and all-out strategic conflict, was built on potentially problematic expectations of proportionality and universally shared conceptions of deterrence. The blurring of conflict across sub-conventional, conventional, and strategic levels as well as the proliferation of actors across that landscape challenge this conceptualization of escalation and call into question its utility. Rather than progressing (more or less) stepwise, with clear thresholds between behavior that would elicit a conventional or nuclear response, crisis or conflict between nuclear-armed adversaries in this new environment is far more complex and unpredictable. And yet, even as academics and policymakers question the representative value of this conceptual ladder, the imagery has proven difficult to shake.

The challenges of managing conflict escalation in today’s strategic environment call for a different metaphor. Drawing from science fiction and physics, the trends described above suggest that alternative and less predictable escalatory pathways are likely and that crisis escalation may instead follow a “wormhole” dynamic. Holes may suddenly open in the fabric of deterrence through which competing states could inadvertently enter and suddenly traverse between sub-conventional and strategic levels of conflict in accelerated and decidedly non-linear ways.7

This article explores three ways in which these wormhole dynamics — fueled by the pursuit of asymmetric advantage, advanced technology, and the diffusion of global power — could unfold between nuclear-armed states. The first section explores the challenges that sub-conventional tactics pose to crisis stability, especially through complex influence campaigns including disinformation and weaponized social media. The second section outlines the unexpected escalatory potential of conflicts that take place along the conventional-nuclear interface where a breakdown of clear firebreaks between a range of technology-enabled strategic capabilities, including warning, surveillance, and communication systems, is blurring the lines between conventional and strategic — including nuclear — domains. The third section examines how sudden, non-linear strategic crises could emerge in a multipolar world of regionally oriented nuclear weapons possessors. The final section discusses both the risks and opportunities these escalatory dynamics may portend for crisis management, arms control, and deterrence.

#### International enforcement’s key.

Suzi Ragheb 21. Legislative intern at EFF. MPA student in Public Affairs at Princeton. BA in Political Science and Government from St. Peter’s. “What About International Digital Competition?”. EFF. Oct 26 2021. <https://www.eff.org/deeplinks/2021/10/what-about-international-digital-competition>

Congress has introduced several competition and anti-trust bills, including a bipartisan package that passed out of committee. The Biden administration has nominated antitrust advocates to key positions: Lina Khan as chair of the Federal Trade Commission, Jonathan Kanter as the Assistant Attorney General for Antitrust at the Department of Justice, and Tim Wu at the National Economic Council. And across the Atlantic, the European Commission is marking up two key pieces of legislation, the Digital Markets Act and the Digital Services Act, that would create new rules for digital services and enhanced competition in the technology sector.

Early this summer and on his first international travel trip, President Biden headed to Brussels to talk about creating a new U.S.EU Tech and Trade Council (TTC) and a Joint Technology Competition Policy Dialogue (JTCPD). There have been few details aside from the initial press releases on what policy approaches would be considered. However, it is a clear sign that there is a transatlantic appetite for tackling competition in the technology space. But what would an international competition policy look like?

International Interoperability and Data Portability Standards

At EFF, we have long advocated for interoperability and data portability as the answers to outsized market power. We believe that creating open standards and allowing users to move their data around to different platforms shifts the market power away from companies and into the hands of consumers. Pursuing this at an international level would be a seismic power shift and would boost innovation and competition.

Having open, interoperable standards between international platforms would allow users to easily transfer their information to the platform that best suits their needs. It would mean that platforms would compete not on the size of their networks, but the quality of their services. When platforms take advantage of network effects, it’s not a competition of offering the best functions, it’s a competition of who can collect the most personal data. The JTCPD would be remiss if they did not address platform and service interoperability, not just ancillary services, as a key part of digital competition.

In an interoperable data world, if you don’t like Facebook’s functions, you would be able to take your data to another platform, one with better services, and you would be able to connect with individuals across platforms.

Given the global nature of the internet, creating international standards would be less burdensome for tech companies, as they wouldn’t have to navigate a patchwork of differing standards. And despite pushback from the platforms, this is not an impossible feat. In fact, interoperability is a cornerstone of the internet. Consider that after Facebook purchased Instagram, the company added chat interoperability between the two platforms, and it plans to make WhatsApp interoperable with both platforms. If we had interoperability standards before the companies merged, the market would have looked and acted differently.

International Antitrust Is Incomplete Without Privacy

Privacy is a fundamental human right recognized by the UN and it must be a part of any international agreement on digital competition. Users today feel hopeless when it comes to their right to online privacy. While interoperability could address privacy concerns by allowing users to self-determine their platform of choice as well as give privacy-conscious platforms the ability to compete on a level playing field with big platforms, there is still a need to establish international privacy standards. Setting a minimum privacy standard pushes companies away from the personal-data-for-profit model that has become inimical to tech monopolies.

In the EU, data privacy standards have been established by the GDPR in 2016, codifying it as a fundamental right with high data protection standards across the EU. The U.S. significantly lags on developing federal privacy standards, despite bipartisan support. Privacy is also a national security concern, as it endangers the welfare of its citizens. A recent report commissioned by the Department of Defense’s Cyberspace Solarium calls on Congress to create national privacy standards as baseline protection against cyberattacks. Setting international privacy standards greatly benefits tech companies. It reduces compliance costs and confusion. And it gives a fair competitive chance to all tech companies, regardless of size.

The Promise of a Truly Competitive Digital Economy Lies in an International Agreement

Otherwise, we create a fractured world for a global internet, rampant with confusion and unequal protection under the law. Under an international agreement, interoperable and portable data standards would be adopted by the industry, leveling the field for both old and new firms. Interoperability will expand opportunities for start-ups to build new tech that works in existing dominant systems. International privacy standards and data minimization enshrines privacy as a human right and pushes the digital market away from the model that relies on personal data exploitation. Creating an international agreement sets up consumers for broader data protections and companies for expanded market access. And a U.S.-EU agreement on tech competition would set the tone for the rest of the globe.

#### Only federal antitrust agencies can enforce internationally.

Pachnou ’17 [Ms. Despina, Organization for Economic Co-operation and Development, “DIRECTORATE FOR FINANCIAL AND ENTERPRISE AFFAIRS COMPETITION COMMITTEE” https://www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/et\_remedies\_united\_states.pdf]

5. The Agencies’ Cooperation with Foreign Jurisdictions on Remedies

18. Achieving effective remedies often entails cooperation with foreign jurisdictions. Such cooperation may allow the U.S. agencies to secure relief that sufficiently protects U.S. competition and consumers without applying the remedy to conduct or assets outside the United States. When an extraterritorial remedy is necessary to address harm or threatened harm to U.S. commerce and consumers, cooperation helps to minimize the risk of conflict with obligations of foreign laws or foreign remedial orders.35 Cooperation and coordination on remedies can be efficient for enforcers and the parties under investigation, especially given that over 130 jurisdictions have antitrust laws and over 80 require pre-merger notification. Cooperation may result in a remedies package that addresses competition concerns in multiple jurisdictions.36 The Agencies work closely with competition enforcers in other jurisdictions on cases under common review, including to help foster convergence and consistent remedy determinations.37

6. U.S. Case Examples

19. To the extent that the Agencies rely on extraterritorial remedies, they do so in both merger and conduct cases, although they arise most frequently in the merger context. In all cases, the Agencies seek remedies that are appropriately tailored and that do not apply extraterritorially unless necessary to address the harm or threatened harm to U.S. commerce or consumers.

6.1. Merger Cases

20. In most mergers, the Agencies can obtain an effective remedy for U.S. competition and consumers without extraterritorial divestitures or other relief. This is the case even when an Agency coordinates with other jurisdictions in investigating a transaction that raises concerns in both domestic markets and markets outside the U.S. Even in these instances, however, coordination between jurisdictions can be helpful. For example, the FTC benefited from coordinating with antitrust authorities in Canada, the EU, and Mexico during the investigation of Emerson Electric Co.’s acquisition of Pentair plc, even though the potential harm to U.S. markets was resolved exclusively through the divestiture of a U.S. switchbox facility.38 Similarly, in the General Electric-Alstom SA merger, effective relief for U.S. markets required divestiture of only U.S. based assets; however, coordination between the Department and the EC in connection with the Department’s investigation “facilitated [the Department’s] investigation and helped formulate remedies that [preserved] competition in the United States and internationally.”39 A coordinated remedy resulted in the Department and the EC announcing separate settlements that eliminated harm to consumers in their respective jurisdictions. 40 There are many more cases in which the Agencies have coordinated with their foreign counterparts on mergers that affect multiple jurisdictions.41

21. Although a merger may affect competition in several jurisdictions, the Agencies focus on preserving competition in the domestic markets that may be harmed by the proposed acquisition. On some occasions, relief secured by foreign jurisdictions means that no remedy, domestic or extraterritorial, is necessary to protect domestic competition. Though our experience in deferring to another authority’s remedy is limited, we have relied on informal deference and remain interested in doing so, under the right conditions. A notable example was in connection with Cisco’s acquisition of Tandberg in 2010. The Department declined to challenge the merger in part due to certain commitments that Cisco made to the European Commission (EC) to facilitate interoperability in products related to a type of videoconferencing called telepresence. Waivers of confidentiality by the parties and industry participants allowed the Department and the EC to cooperate closely in their parallel reviews of the transaction, resulting in an efficient outcome for the enforcers and the merging parties.42

22. Nevertheless, certain merger investigations resolved by consent decree have required the divestiture of assets located outside the United States to preserve competition within the United States. For example, the FTC consent decree resolving concerns regarding the merger of cement manufacturers Holcim Ltd. and Lafarge SA required, in part, divestiture of a Canadian cement plant and related U.S. terminals along with two Canadian terminals related to a U.S. cement plant. The FTC explained that the divested assets “remedy competitive concerns in northern U.S. markets [and are] part of a larger group of Holcim assets located in Canada that Holcim and Lafarge have agreed to divest to address competitive concerns raised by the [Canadian Competition Bureau (“CCB”)]. Commission staff worked closely with staff from the CCB to reach outcomes that benefit consumers in the United States.”

43 An extraterritorial remedy was also required to resolve Department’s investigation of the Anheuser-Busch InBev SA/NV & Grupo Modelo S.A.B. merger. The consent decree in that matter similarly required divestiture of a facility outside of the United States, the Grupo Modelo brewery in Mexico, and a perpetual and exclusive U.S. trademark license to the seven brands of beer that Modelo then offered in the United States, as well as three brands not yet offered in the United States, but currently sold by Modelo in Mexico. This remedy allowed the acquirer “to meet current and future demand for Modelo Brand Beer in the United States,” which resolved concerns that the merger would harm competition in twenty-six local U.S. markets.

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

Robert Scammell 21. Deputy Editor at Verdict. “Big Tech’s smart city power grab”. Verdict Magazine. Issue 9. May 2021. 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.

Bengt Ahlgren et. al 16. Senior researcher in the Decisions, Networking, and Analytics (DNA) lab at SICS Swedish ICT, PhD in Computer Systems from Uppsala. Markus Hidell, associate professor in communication systems and at the Network Systems Laboratory (NSLab) at the KTH Royal Institute of Technology, PhD in Telecommunication from 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 from the Chinese University of Hong Kong. “Internet of Things for Smart Cities: Interoperability and Open Data”. IEEE Internet Computing. Nov/Dec 2016. <http://user.it.uu.se/~eding810/journals/Internet-of-Things%20for%20Smart%20Cities%20Interoperability%20and%20Open%20Data.pdf>

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.

Julian Cribb 16. Senior Visiting Fellow at FutureDirections, former scientific editor for The Australian, author of *The Coming Famine* and *Poisoned Planet*, former foundation president of the Australian Science Communicators Association. “The Urbanite (Homo urbanus)”. Chapter in *Surviving the 21st Century*, pp. 147-169. 2016. https://link.springer.com/chapter/10.1007/978-3-319-41270-2\_8

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.

#### FTC adjudication under Section 5 is key. Their expertise and investigatory power allow them to identify all forms of interoperability restrictions in an ever-changing market.

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].

IV. Section 5 in Theory and Practice

Section 5's origin story contains all the ingredients to make it the ideal interoperability enforcement vehicle: a broad congressional mandate, consumer input, expert investigatory powers, and extrajudicial punitive measures. Congress, frustrated with the stagnant progress of antitrust enforcement under Sherman, wrote Section 5 with language intentionally more expansive than the Sherman and Clayton Acts 162 to [\*478] permit the FTC to address the changing economic landscape and to rectify threats to competition on a case-by-case basis. 163Specifically, Section 5 provides that "the Commission is hereby empowered and directed to prevent persons ... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 164 This broad mandate in conjunction with the FTC's special norms-setting duties 165 allows the FTC to respond to changing economic environments and to account for unique attributes of nuanced industries, like software development for the Internet. 166With the passage of Section 5, Congress signaled faith in the FTC's singular ability to navigate complicated or frontier antitrust matters although both the FTC and DOJ have the authority to bring cases under Sherman and Clayton Acts, only the FTC can enforce Section 5. 167

Congress intentionally designed the FTC and its authorities to help it appropriately define the contours of "unfair methods of competition" and "unfair or deceptive acts or practices." Congress imbued the FTC rulemaking and adjudicatory authority, granting broad discretion to make rules with the force of law or challenge impermissible conduct where deemed appropriate. 168This role was enhanced by the Commission's design as a combination research, policy, and enforcement agency. It, in theory, enjoys the support of leading experts, originally in the field of economics but now increasingly in the fields of science and technology as well and is led by Commissioners who serve [\*479] for seven years, which "give them an opportunity to acquire" the expertise needed to determine what constitutes a Section 5 violation. 169 The Commission maintains one of the most extensive consumer protection complaint databases, 170 crowdsourcing data to inform enforcement priorities from the very constituents competition law is intended to serve. When suspicious of a Section 5 violation, the FTC is granted "broader powers of investigation than almost any other department or agency in the federal government." 171In sum, the FTC is a unique regulatory body and has several tools at its disposal to carry out its charge.

Over the years, the FTC has interpreted Section 5 to establish two agency goals: protecting competitive structures and protecting consumers. 172Today, the FTC is divided into three major bureaus: the Bureau of Competition, the Bureau of Consumer Protection, and the Bureau of Economics. The Bureau of Competition (BC) and Bureau of Consumer Protection (BCP) are the enforcement arms for the FTC's corresponding dual statutory mandate, while the Bureau of Economics consists largely of economists who provide the analytical basis for the legal theories of its counterparts. 173Both enforcement bureaus conduct investigations, consult experts, and make recommendations to the Commission as a whole regarding viable enforcement actions to pursue. 174 They are well suited to seize the opportunity of regulating API design to disallow overly restrictive APIs that contravene the goals of competition law.

[\*480]

A. Rulemaking v. Adjudication

Of the two enforcement tools the agency has been given adjudication and rulemaking adjudication is the only feasible avenue for effective regulation. Rulemaking authority refers to the Commission's ability to "define with specificity" which acts or practices are unfair through formal or informal rules that have the force of law. 175Although Congress technically handed the FTC rulemaking power in connection with Section 5 enforcement, it has since made rulemaking, whether for promoting permissive APIs or otherwise, essentially impracticable. Congress has limited, by statute, the industries and activities about which the FTC is permitted to pass rules 176 and imposed requirements above and beyond those in the Administrative Procedures Act (APA). 177Even without rulemaking in its toolkit, the FTC can still rely on adjudicative proceedings to address overly restrictive API designs that it suspects violate principles of competition law and consumer protection.

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

Although FTC adjudication under novel theories was previously met with disdain from Congress and the courts, recent cases suggest a slightly heightened level of deference awarded to agency findings. Congress responded to periods of substantial FTC activity in consumer harm cases with restrictive action, limiting the Commission's ability to [\*482] interpret its broad mandate. 184Similarly, the Commission experienced appellate rebuke over a series of cases signaling a lack of deference given to the agency's conclusions. 185 Since Chevron, however, courts have shown the FTC a slightly enhanced level of deference regarding its decision-making. 186 In the first judicial review of a Section 5 action since Chevron, the court was unable to review the question of deference given the suit's posture, 187but in a Sherman-based FTC suit, the Supreme Court did acknowledge deference owed to the Commission's finding of fact in language that was not cabined to just Section 1 and 2 claims. 188 However, most lower courts still don't give the FTC interpretations of Section 5 Chevron deference, using language that alludes to a lower Skidmore/Seminole Rock standard of deference. 189Either way, the FTC's actions to encourage business behavior are practically [\*483] immune, as seen in the Commission's ability to motivate Google to alter its search result practices by conducting a full investigation but never filing a formal complaint. 190

B. Unfair Methods of Competition

Practices that smell of antitrust but do not pass muster under traditional antitrust law's stringent tests can fall within Section 5's competition purview as long as they violate the spirit and policies of traditional antitrust laws. 191 The FTC has consistently interpreted "unfair methods of competition" to "encompass[] not only those acts and practices that violate the Sherman or Clayton Act but also those that contravene the spirit of the antitrust laws and those that, if allowed to mature or complete, could violate the Sherman or Clayton Act." 192 [\*484] This permits the FTC to bring actions against companies for beginning courses of action that have not yet manifested in substantial harm to competition, which can encompass the various theories of harm discussed earlier in Section II(c)(ii) that did not violate the letter of the law, but might be likely to mature into an outright violation. Incipient harm is a theory of enforcement that relies on the penumbras of antitrust law to halt anticompetitive practices and monopolies in their formative stages. 193

[\*485] Accordingly, the Agency brings enforcement actions under Section 5 that do not amount to Section 1 or 2 violations, using theories of invitations to collude and breach of agreements to disclose information critical to meeting an industry standard. Both theories constitute incipient instances of anticompetitive behavior that the FTC acts to restrict early on for their clear potential to injure the marketplace. Invitations to collude invoke many of the same theories of harm relevant to horizontal mergers but encompasses a greater range of transactions that are not merger specific. Failure to disclose information related to compliance with an industry standard appears similar to theories of harm found in vertical mergers, namely the flexing of market dominance by one company in denying competitors the opportunity to achieve interoperability with its product. These precedents suggest that the FTC may be able to bring actions against API redesigns that either act as collusive collaborations among competitors to the exclusion of others or as the unfair exertion of dominant influence by one player against others that relied on said APIs to achieve previously agreed upon interoperability standards.

The FTC has challenged invitations to collude in shared monopolies not only when parties collaborate but also when they act in concert. 194In shared monopoly enforcement cases, the Commission did not require each player to possess a dominant market share (relevant under a Section 1 claim) or the existence of an agreement (relevant to a Section 2 claim) in challenging the unilateral action. 195Instead, the [\*486] FTC asks whether "the practice in question unfairly burdened competition for a not insignificant volume of commerce." 196For example, the FTC's complaint in the 2000 SonySection 5 enforcement action focused primarily on the collective shares of the five players alleged of passive collusion which amounted to 85 percent of the total market and whether the concurrent behavior had the "same practical effect" as a minimum price agreement. 197Similarly, eBay and Amazon comprise the vast majority of the domestic e-commerce marketplace, a shared monopoly. 198So, if they conditioned access to their APIs on receiving high commission rates, the FTC can argue that the platforms are restricting competition in a shared monopoly scheme, whether they overtly colluded or simply acted in parallel.

[\*487] Invitation to collude cases can also extend to business decisions by market dominant players to share high value information with a limited group of competitors. 199 Exclusive access to confidential business information does not amount to exclusive dealings but does provide incredible competitive advantage to recipients that other players cannot bargain for in the marketplace, amounting to anticompetitive unilateral action. 200In the context of Internet businesses, companies with closed APIs can decide to interact with other large market players only, similarly denying the opportunity for smaller or newer members to the market to negotiate entry into the collaboration. Recently, The New York Times discovered that Facebook, a dominant market player but not a monopoly, gave Spotify, Microsoft, Amazon, and others exclusive access to user data through restrictive APIs, permitting these hand-selected companies to benefit from its sensitive business intelligence to the detriment of their competitors. 201

The FTC has also challenged refusals by dominant players to abide by information-sharing agreements that foster interoperability. These cases are premised on the existence of standard-setting organizations (SSOs) and the protection of the information in question by a patent or other form of intellectual property right. 202SSOs are procompetitive entities that create structured, mutually beneficial relationships [\*488] between interdependent businesses. 203For instance, camera companies who would otherwise keep the mechanics of their products secret enter into contracts with competitors to generate and abide by certain design standards to ensure that all cameras are compatible with the film available on the market. It is usually in a company's best interest to protect trade secrets, but this is outweighed by the benefits of ensuring their product is compatible with as many complementary products on the market as possible. 204SSOs allow consumers to buy Canon, Nikon, or Fujifilm cameras and use the same standard Kodak film with all of them, to the benefit of all competitors. Similar to proprietary film design, APIs also constitute intellectual property that companies tend to withhold but can share to their advantage. The same "procompetitive potential of standard-setting activities" exists for designing permissive APIs and building third party reliance on them, and these APIs certainly develop "a standard [that] may displace the normal give and take of competition." 205

The FTC has the flexibility to expand its understanding of this claim to include refusals to disclose information without the existence of a formal agreement or patent, under theories akin to promissory estoppel or reliance interests built. 206 The diffuse nature of the Internet marketplace frustrates the ability to enter formal contracts or form [\*489] SSOs. 207However, the theory of harm underpinning these enforcement actions can extend to restrictive API redesigns that break interoperability between previously reliant third parties. In a case against Dell, the FTC focused on the harm of Dell's refusal to share information relied on by third parties when designing their products to be interoperable with Dell as well as the potential chilling effect Dell's actions could have on willingness to join SSOs. 208 Holding API creators to the representations they make implicitly through API design or explicitly in documentation would prevent them from reneging after reaping the benefits of the representation. This may also act to deter designing APIs ex ante that are too permissive to maintain in the long term, avoiding the reliance interests before they attach. 209

Finally, the FTC remains active in investigating anticompetitive behavior under theories akin to incipient tying, 210even if these suits do not always result in formal administrative action. Often, dominant players condition the use of their API on agreements not to engage in certain practices that would be detrimental to the dominant player. Incipient tying, unlike complete bars to entry, does not make a program wholly unavailable but rather "imposes ... incremental costs on customers who use rival" products. 211In United States v. Microsoft, the DOJ challenged the manner in which Microsoft used various methods to tie its middleware, Internet Explorer, to its operating system, Windows, 212in an API redesign that "lacked any technical or business [\*490] justification." 213But Section 5 claims need not satisfy traditional antitrust tests. 214Indeed, the FTC brought a Section 5 claim against Intel under similar API interoperability theories, arguing that the company's software redesign that made complementary products prefer its CPUs over others on the market was intended solely to reduce competition with no consumer benefit justification. 215

This theory could extend to cases of restrictive APIs that condition access on agreement to an unrelated term, such as the use of or refusal to use a separate product. For example, Uber conditions the use of its API on an agreement from the user not to use the API for applications providing real time price comparisons with competitors a condition that "deprives the public of the advantages that flow from free competition." 216More recently, the FTC investigated Google's potentially anticompetitive behavior, though no complaint was formally brought. 217The investigation evinced a continued concern with the company using its market dominance to its own benefit. 218Namely, Google allowed others to be listed in search results through an API but purportedly artificially curated the platform's search results to benefit its own subsidiaries over organic results, practically tying successful [\*491] use of the API with being financially tied to the company. 219Additionally, Google conditioned the use of its AdWords API on the refusal to use third party products that allow consumers to manage multiple ad campaigns with AdWords competitors through one streamlined interface. 220The inquiry considered the anticompetitive effects of these actions but primarily hinged on Google's intent in API design was its goal to injure competition or improve its platform for users? 221Ultimately, the Commission was able to apply such substantial pressure that Google agreed to alter both practices with more permissive APIs. 222 The FTC can use its broad investigative powers to uncover these practices that would otherwise go unnoticed by most consumers and put pressure on the company to improve access without formally threatening enforcement.

#### Adjudication remedies avoid litigation and set clear, industry-wide norms.

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].

E. Proactive Remedies

The FTC can play a powerful role as a norm-setting body in the government, defining evidence-backed standards to promote competition and protect consumer welfare through investigations into business practices and consent decrees, without resorting to lengthy and expensive litigation. The Commission is well positioned to counter the potentially anticompetitive instincts of a concentrated Internet marketplace using its remedial toolkit without causing harm to business or chilling the marketplace. Data security enforcement examples serve as a strong example of the manner in which initiating Section 5 proceedings can: (1) notify parties of potentially anticompetitive behavior, 272(2) negotiate a proactive plan to mitigate the risk of harm, 273 and (3) signal to the remaining players in the market the principles underlying the enforcement action. 274

First, the FTC can act to halt API redesigns before they ossify into new code through cease and desist orders, avoiding the problem of "scrambling the egg" in the first place while the potentially anticompetitive practice is investigated. 275 These orders can be seen as the administrative agency equivalent of an injunction, and the agency can seek civil penalties and injunctions for violations of these orders. 276 Then, the harm is rectified through consent decrees, or prescriptive [\*504] agreements setting forth strict conditions when the Commission has "reason to believe" that a company has violated Section 5 and the company wants to avoid litigation. 277To ensure compliance, consent decrees generally require periodic internal audits and, in extreme cases, internal monitors to oversee implementation of the order's conditions. 278 These aggregate orders begin to shape the contours of Section 5 violations and espouse foundational principles informing the enforcement actions, functioning much like common law doctrine. 279

The process by which these decrees are finalized preserves public participation in norms setting, ameliorating the concern that courts are ill suited to adjudicate nuanced issues of technology and business. Some find these consent decrees unduly powerful, enabling the FTC to extract commitments from companies when they would not be able to win in litigation. 280But consent decrees are not examples of unilateral agency rule but rather byproducts of a fairly open and collaborative process. The content of these consent decrees do not operate like Oz, hidden behind veils of ignorance. Rather, the decrees are made public and include a 30 day period for public comment before the order is finalized, allowing FTC constituents (the consumers and competitors in that market) to have a say in remedial measures. 281Further, in establishing these norms, the FTC does not divine industry standards as the Oracle of Delphi but rather looks to consumer expectations and industry best practices. 282Therefore, the FTC is less of a norm-setter than a norm-enforcer in cases when the market does not serve to enforce these norms itself.

[\*505] Consent decrees are powerful examples of forward-looking remedies that can both neutralize a competition harm or consumer harm while also providing better guidance to future actors. They can also serve as exceptions to the principle that companies owe their competitors no duty of aid. 283For example, the consent decree in the antitrust case against Microsoft, involving APIs and interoperability, set forth conditions that required Microsoft to undertake the cost and effort of developing more interoperable APIs and making documentation of their APIs publicly available to ensure that all competitors had fair opportunity to make their products compatible with the Microsoft operating system. 284The consent decree went as far as to force specific business transactions, requiring Microsoft to license its intellectual property to firms developing interoperable technologies. 285This imposed a cost on Microsoft to ensure that all programs could integrate with Windows in the same way that Microsoft's own products could. 286 Similar consent decrees can encourage internet businesses with comparable market dominance to Microsoft in the 90s to bear the cost of redesigning their APIs for improved interoperability.

However, FTC remedies are not without shortcomings. The Commission is effectively unable to ensure that adjudicative outcomes are accommodated by defendants and other market players because Section 5 does not provide for civil penalties as a first order tool. 287 [\*506] This detracts from the Commission's ability to deter because enforcement of a consent decree requires bringing another resource-intensive suit challenging noncompliance. Moreover, a circuit recently challenged the agency's authority to include proscriptive requirements for information security in a data privacy challenge under Section 5, stating that a cease and desist order must demand a company to halt an ongoing activity but cannot preemptively require it to engage in activities prescribed by the FTC. 288Aware of its own tenuous enforcement capabilities, the FTC specifically raised questions about the scope of its remedial authority during the recent 2018 hearings. 289

V. Conclusion

Harm from anticompetitive practices can occur in degrees, and activity that does not rise to the level of traditionally proscribed antitrust behavior can still injure market innovation and consumers. The Internet is still fledgling and has yet to establish concrete norms, which provides a unique opportunity for a norm-building agency to engage with market players, using its unique procedural and structural advantages to help shape these norms in utility-maximizing ways. This is especially true for the regulation of API design in an Internet environment that is growing increasingly concentrated because marketplace conditions do not incentivize cooperation between a large number of diverse players. Rather, they incentivize increased market concentration through the redesign of APIs in more and more restrictive fashions. If the unification of the three largest online social media communication platforms seems concerning on its face, then there should be an avenue to investigate those suspicions further.

#### Certainty and federal action are key – a thicket of legal defenses discourages 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. “Unfair Use: Anti-Interoperability and Our Dwindling Digital Freedom”. The Reboot. Apr 13 2021. <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.

### plan – 1ac

#### Thus, the plan: The United States federal government should prohibit unfair methods of competition by digital platforms that restrict interoperability.

### middleware advantage – 1ac

#### Advantage two is *middleware*.

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

Francis Fukuyama 21. Mosbacher Director of Stanford’s Center on Democracy, Development and the Rule of Law. Director of the Ford Dorsey Master's in International Policy at Stanford. PhD, political science, Harvard. “Making the Internet Safe for Democracy”. Journal of Democracy, Volume 32, Number 2, April 2021, pp. 37-44. https://muse.jhu.edu/article/787834/pdf?casa\_token=VdaYtO26fNMAAAAA:aM5-x7m0oZADeR-FmoDEVkwwyKzCw2-uzMpN3dxf92QDv6FDYmwObGP6bze5Rmd\_lsg5XiFkN3t\_

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’s key – dominant platforms have no incentive to police information.

Francis Fukuyama 21. Mosbacher Director of Stanford’s Center on Democracy, Development and the Rule of Law. Director of the Ford Dorsey Master's in International Policy at Stanford. PhD, political science, Harvard. “Making the Internet Safe for Democracy”. Journal of Democracy, Volume 32, Number 2, April 2021, pp. 37-44. https://muse.jhu.edu/article/787834/pdf?casa\_token=VdaYtO26fNMAAAAA:aM5-x7m0oZADeR-FmoDEVkwwyKzCw2-uzMpN3dxf92QDv6FDYmwObGP6bze5Rmd\_lsg5XiFkN3t\_

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.

Francis Fukuyama 21. Mosbacher Director of Stanford’s Center on Democracy, Development and the Rule of Law. Director of the Ford Dorsey Master's in International Policy at Stanford. PhD, political science, Harvard. “Making the Internet Safe for Democracy”. Journal of Democracy, Volume 32, Number 2, April 2021, pp. 37-44. <https://muse.jhu.edu/article/787834/pdf?casa_token=VdaYtO26fNMAAAAA:aM5-x7m0oZADeR-FmoDEVkwwyKzCw2-uzMpN3dxf92QDv6FDYmwObGP6bze5Rmd_lsg5XiFkN3t_>

\*Size 4 text is all AFF and cut in the Fukuyama card above – I just wanted to retain the international examples at the top and bottom of the card for this one.

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.

#### Democracy caps all existential risk.

George Eaton 20. Senior online editor of the New Statesman. Citing Noam Chomsky, Laureate professor in the Department of Linguistics at the University of Arizona and professor emeritus at MIT, Ph.D. in linguistics from Penn. “Noam Chomsky: The world is at the most dangerous moment in human history”. The New Statesman. Sept 17 2020. 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.”

#### DPT is empirical law.

Kosuke Imai and James Lo 21. Professor of Government and of Statistics at Harvard University. Assistant Professor of Political Science at the University of Southern California. “Robustness of Empirical Evidence for the Democratic Peace: A Nonparametric Sensitivity Analysis”. International Organization 75, Summer 2021, pp. 901–19. https://imai.fas.harvard.edu/research/files/dempeace.pdf

The democratic peace — the idea that democracies rarely fight one another — has been called “the closest thing we have to an empirical law in the study of international relations.” Yet, some contend that this relationship is spurious and suggest alternative explanations. Unfortunately, in the absence of randomized experiments, we can never rule out the possible existence of such confounding biases. Rather than commonly used regression-based approaches, we apply a nonparametric sensitivity analysis. We show that overturning the positive association between democracy and peace would require a confounder that is 47 times more prevalent in democratic dyads than in other dyads. To put this number in context, the relationship between democracy and peace is at least five times as robust as that between smoking and lung cancer. To explain away the democratic peace, therefore, scholars must find far more powerful confounders than already those identified in the literature.

#### Disinformation spread by platforms’ content algorithms enables far-right terror groups to recruit terrorists and coordinate CBRN attacks.

Gabriel Weimann and Natalie Masri 20. Professor of Communications at the University of Haifa, former fellow at the Woodrow Wilson International Center for Scholars, author of *Terrorism in Cyberspace: The Next Generation*. Economic Empowerment Consultant for the U.S. Chamber of Commerce Foundation's Corporate Citizenship Center. “The Virus of Hate Far-Right Terrorism in Cyberspace”. March 2020. IDC Herzliya. <https://www.ict.org.il/images/Dark%20Hate.pdf>

The Rise of Far-Right Terrorism

Far-right violence and terrorism are a growing threat to Western societies. Far-right terrorist attacks increased by 320 per cent between 2014 and 2019 according to the 2019 Global Terrorism Index. In 2018 alone, far-right terrorist attacks made up 17.2% of all terrorist incidents in the West, compared to Islamic groups which made up 6.28% of all attacks. In January 2019, the Anti-Defamation League’s Centre on Extremism reported that every extremist killing in the US in 2018 was linked to far-right individuals or organizations. German authorities registered 8,605 right-wing extremist offenses including 363 violent crimes in the first half of 2019. Compared to the first half of 2018, an increase of 900 far-right crimes was recorded during the same period. Far-right terrorism is on average five times deadlier than far-left terrorism, with an average of 0.92 deaths per attack compared to farleft terrorism with 0.17 deaths. Nineteen countries across North America, Western Europe and Oceania have been targeted by far-right attackers. This trend in far-right attacks has led some observers to state that far-right domestic terrorism has not been treated seriously enough in the West and that security and intelligence services should pay closer attention to this emerging threat.

“Far-right” refers to a political ideology that centers on one or more of the following elements: strident nationalism (usually racial or exclusivist in some fashion), fascism, racism, antiSemitism, anti-immigration, chauvinism, nativism, and xenophobia. Far-right groups are usually strongly authoritarian, but often with populist elements and have historically been anti-communist, although this characteristic has become less prominent since the end of the Cold War. Not all groups or organizations with any one of these characteristics can be considered far right, and not all farright groups are automatically violent or terroristic. However, terrorist groups with these characteristics and individuals sympathetic to these ideals have been classified as “far-right terrorism”.

Far-right terrorists have a strong inclination to change the established order and favour traditional aptitudes (typically white, heterosexual and Christian) and advocate the forced establishment of authoritarian order. Far-right attacks are also less predictable as perpetrators are typically unaffiliated with a terrorist group, making them harder to detect. Far-right extremists have also shown a long-term interest in acquiring Chemical, Biological, Radiological and Nuclear (CBRN) weapons, resulting in several CBRN far-right terrorist plots in Western countries (mostly in the U.S.) which fortunately did not come to fruition. Another development is the phenomenon of individuals taking part in extreme right-wing terrorist plots without previous contacts to the extremist environment, sometimes described as “Hive Terrorism”. All the above appears to show a significant terrorist threat posed by extreme right-wing activists and groups.

The Propaganda of Far-Right Terrorism

Like many other modern extremists, jihadists and terrorists, the far-right relies on a massive and wide-ranging propaganda machinery. The propaganda campaigns allow the far-right to maximize media and online attention while limiting the risk of individual exposure, negative media coverage, arrests and public backlash. The barrage of propaganda attempts to normalize extremist messages and bolster recruitment efforts while targeting minority groups including Jews, Blacks, Muslims, non-white immigrants and the LGBTQ community.

The media presence of the far-right is becoming more common across Europe and North America. The award-winning report by Horaczek (2019) reveals several stages in the media strategy of the far-right:

1. Build your own media empire

2. Stoke fear and doubt through fake news (disinformation)

3. Defame your critics

4. Use social media as an amplifier

5. Put the freedom of the press under pressure.

Extreme right activists and their ilk have long used propaganda as a tool to spread their message. Long before the Internet, they distributed hateful flyers or drove from town to town, leaving their hateful papers, brochures and manifestos on front steps and in driveways. These methods are still in use: in 2019, for example, U.S. white supremacists used more paper-canvassing of neighborhoods and college campuses than at any other time in years, with an unprecedented number of flyers, banners, stickers and posters appearing across the country (ADL, 2020).

The most effective propaganda strategy of the Far-right is the use of disinformation. Disinformation has been a matter of state since politics began, with propaganda used by rulers, governments and their intelligence agencies to influence the political landscape both at home and abroad. But disinformation has been, mostly, the privilege of those in power. Today, the rise of digital platforms has changed this and now fringe groups, malevolent actors and extremists have access to platforms that can proliferate disinformation and stir resentments of all kinds. According to a special study conducted by The Investigate Europe team (2019), “There are plausible arguments to link the rise of the Neo-nationalists in the US and across Europe with this new phenomenon”.

A new development in the propaganda campaigns launched by the far-right was the adaption and use of new media: the rise of online media has created new opportunities for communication, organization and mobilization by far-right-wing extremist and right-wing radical political groups. Whilst right-wing extremists exploit online platforms and social media for political purposes, the extent to which they have abused online communication is far less certain.

The Attraction of Online Platforms

The far-right's online presence had developed over three decades, using bulletin board systems, websites, online forums, and more recently, social media (Burris et al. 2000, Back 2002, Zickmund 2002). Social media has “algorithmically amplified, sped up and circulated a political backlash by White voters that the alt-right has exploited...,making extreme viewpoints more tolerable in public discourse”(Daniels 2018, pp. 64–65). As Ganesh (2020) argues, much of the far-right groups' ability to manipulate public discourse is due to their adoption of the practices and aesthetics of misogynist, trolling, and gaming subcultures, where they have honed their ability to use text, memes, and videos to use emotional appeals and encourage participation with anti-immigrant and white supremacist discourse.

The growing presence of extremists groups in cyberspace is at the nexus of two key trends: the democratization of communications driven by user-generated content on the Internet, and the growing awareness of modern vigilantes of the potential of the Internet for their aims. Terrorists have used the Internet, as several studies have revealed, for numerous purposes (Weimann, 2006; 2016a). They use the Net to launch psychological campaigns, recruit and direct volunteers, raise funds, incite violence and provide training. They also use it to plan, network, and coordinate attacks. Thus, not only has the number of terrorist online platforms increased but also the ways in which terrorists use the Internet has diversified.

The network of computer-mediated communication (CMC) is ideal for extremists-ascommunicators: it is decentralized, cannot be subjected to control or restriction, is not censored and allows free access to anyone who wants it. The typical, loosely knit network of cells, divisions, and subgroups of modern extremist organizations finds the Internet both ideal and vital for interand intra-group networking. The great virtues of the Internet—ease of access, lack of regulation, vast potential audiences, fast flow of information, and so forth—have been converted into advantages for groups committed to terrorizing societies to achieve their goals. The anonymity offered by the Internet is very attractive to modern radicals, terrorists and vigilantes. Because of their extremist beliefs and values, these actors require anonymity to exist and operate in social environments that may not agree with their particular ideology or activities. The online platforms, from websites to social media and the Dark Net, provide this anonymity and easy access from everywhere with the option to post messages, to e-mail, to upload or download information and to disappear into the dark.

These advantages have not gone unnoticed by far-right groups, who moved their communications, propaganda, instruction and training to the cyberspace. As Hoffman and Ware (2019) concluded, ‘today’s far-right extremists, like predecessors from previous generations, are employing cutting-edge technologies for terrorist purposes’. The far-right online presence is not restricted to a single online platform or space but is instead a patchwork of various types of platforms and spaces, from websites to social media and even the Dark Net. Far-right extremists are generating their content on a variety of online platforms and increasingly also utilizing a wider range of new media technologies for their purposes. A range of relatively new and highly accessible communication ‘applications’ is another component of this trend. Many of these newer technologies fit into the category of so-called ‘dark social’, which refers not to the ‘dark’ nature of the content but to the difficulties of tracking content and communicators. Let us review the variety of online platforms and their use by the far-right terrorists.

The Far-Right on Social Media

YouTube

For a short time on January 4, 2018, the most popular live-streamed video on YouTube was a broadcast dominated by white nationalists. The debate topic was scientific racism, which they referred to as “race realism”—a contemporary incarnation of the long-standing claims that there are measurable scientific differences between races of humans. Arguing in favor of scientific racism was infamous white nationalist Richard Spencer, known for having popularized the term “alt-right”. During the broadcast, the video became the #1 trending live video worldwide on YouTube, with over 10,000 active viewers. The archived version of the broadcast has been viewed an additional 475,000 times.

YouTube is a video-sharing platform, operating as one of Google's subsidiaries. YouTube allows users to view and upload video clips, to rate, share, add to playlists, flag, report, comment on videos, and subscribe to other users. It offers a wide variety of user-generated and corporate media videos. YouTube has around 2 billion daily users, most of them are young, hence appeals to those without fully formed political beliefs are likely to become influenced by persuasive communication. YouTube is more popular amongst teenagers than Facebook and Twitter. As of May 2019, over 500 hours of video content are uploaded to YouTube every minute. Based on reported quarterly advertising revenue, YouTube is estimated to have US$15 billion in annual revenues.

Video platforms such as YouTube are frequently used by extremists to propagate their views, spread hate and even live-stream attacks. Aimless young men, usually white, visit YouTube looking for direction or distraction and are seduced by a community of far-right propagandists. Some young men discover far-right videos by accident, while others seek them out. A common feature in many of these cases is YouTube and its notorious algorithm, the software that determines which videos appear on users’ home pages. The problem of YouTube’s algorithm is that it promotes fringe beliefs, lewd and violent videos, conspiracy theories and extremist ideas. A user could start with a leftleaning video on racism and slowly but surely end up, through a series of recommendations, watching right-wing extremist content. Far-right YouTubers have learned to exploit the platform's algorithm and land their videos high in the recommendations of less extreme videos.

YouTube has been a useful recruiting tool for far-right extremist groups. Bellingcat, an investigative news site, analyzed messages from far-right chat rooms and found that YouTube was cited as the most frequent cause of members’ “red-pilling” -an online slang term for converting to far-right beliefs (Evans, 2018).

A European research group, VOX-Pol, conducted a separate analysis of nearly 30,000 Twitter accounts affiliated with the alt-right. It found that the accounts linked to YouTube more often than to any other site (Berger, 2018). A study on online radicalization analyzed 331,849 videos on some 360 channels (Ribeiro et al. 2020). The study found “strong evidence for radicalization among YouTube users”, citing how users who consume extreme far-right content had previously consumed content affiliated with the so-called intellectual dark web and the alt-lite. Referring to YouTube, the study concluded: “Our work resonates with the narrative that there is radicalization pipeline”. Similar findings were presented at the ACM FAT 2020 Conference in Barcelona, supporting the notion that YouTube’s platform is playing a role in radicalizing users via exposure to far-right ideologies (Lomas, 2020). The study, carried out by researchers at Switzerland’s Ecole Polytechnique Fédérale de Lausanne and the Federal University of Minas Gerais in Brazil, found evidence that users who engaged with a middle ground of extreme right-wing content migrated to commenting on the most fringe farright content.

Finally, a report from Data & Society found that “YouTube, a subsidiary of Google, has become the single most important hub by which an extensive network of far-right influencers profit from broadcasting propaganda to young viewers” (Lewis, 2018).

Facebook

Facebook is the third most visited website on the Internet and the world’s largest social media network with over 2.2 billion regular users as of February 2018. Because of its popularity, Facebook has become an important tool for political or community organizations and commercial brands—including, unfortunately, far-right extremists. Even though the company explicitly bans hate speech and hate groups in its Community Standards, Facebook appears to encounter a real challenge regarding the removal of neo-Nazi and white supremacist content from its platform.

At around 1:30 p.m. on a Friday afternoon, people around the world watched the streaming video of a mass murder in Christchurch, New Zealand. The attacker, Brenton Tarrant, had announced he would carry out a deadly attack and stream it live on Facebook. The first fans quickly voiced their support. “Good luck,” one user wrote; another: “Sounds fun.” A third person wrote that it was the “best start to a weekend ever”. Around 200 Facebook users watched through their smartphones, tablets or computers as the murderer got out of his car, opened his trunk where he kept his weapons and began killing 50 people in and around two mosques. The power of social media, especially Facebook, turned the terrorist attack in Christchurch into a twisted act of terrorist performance, designed to inspire imitation and emulation elsewhere. The attacks were livestreamed for 17 minutes and viewed at least 4,000 times before Facebook took down the link. Over the next 24 hours, Facebook removed another 1.5 million copies of the attack video from its pages. In the aftermath of the Christchurch attack, social media has played a critical role in capitalizing on the event. An ISIS-linked posting demanded that fellow ISIS supporters “logon to Facebook and Twitter and incite for shedding the blood of the worshippers of the Cross”.

Rublin (2019) studied the Facebook connection between far-right groups and pro-Palestinian groups who support the BDS (Boycott, Divestment, and Sanctions) against Israel. The study revealed several neo-Nazi white supremacists who actively participate in several BDS and pro-Palestinian Facebook groups and use them as a platform. These Facebook users publicly post blatant antiSemitic material, both on their personal pages and in these Facebook groups. They evoke classical anti-Semitic myths and imagery, Christian lore, and Nazi-era propaganda and modern anti-Semitic tropes. The rejection of Zionism and the State of Israel and support for the BDS against Israel and the Palestinian cause is associated with the deep-seated anti-Jewish views of these individuals. Although most of their posts express mere vilification, demonization, and hatred, we have seen some public calls for action against Jews and Judaism.

Facebook attempts to fight the abuse of the service by extremists and removed 18 million examples of “terrorism content”, using expertise and artificial intelligence, as well as other tools such as video-matching technology and language detection. Yet, Facebook is losing the fight: in September 2018, the Counter Extremism Project (CEP) identified and monitored a selection of 40 Facebook pages that sell white supremacist clothing, music, or accessories, or represent white supremacist or neo-Nazi groups. CEP researchers recorded information for each page such as the number of likes, date of creation, and examples of white supremacist or neo-Nazi content. After two months, CEP reported the pages to Facebook, but 35 of the 40 remained online. As the report concludes, “Clearly, Facebook’s process for reviewing and removing this content-which violates its Community Standards is inadequate” (CEP, 2019, p.2).

Facebook has also failed to stop a coordinated far-right operation profiting from disinformation and anti-Islamic hate almost two months after it was publicly exposed. A network of Facebook’s largest far-right pages were part of a coordinated commercial enterprise, prompting promises from the social media giant that it would crack down on the network. The British paper The Guardian investigated these Facebook postings and revealed a covert plot to control some of Facebook’s largest far-right pages and harvest Islamophobic hate for profit (The Guardian, 2019).

A web of far-right Facebook accounts spreading fake news and hate speech to millions of people across Europe has been uncovered by the campaign group Avaaz, an online activist organization. The search revealed over 500 far-right groups and Facebook pages operating across France, Germany, Italy, the UK, Poland and Spain. Most were spreading fake news or using false pages and profiles to artificially boost the content of parties or sites they supported, in violation of Facebook’s rules. The Facebook postings ranged from French accounts sharing white supremacist content, to posts in Germany supporting Holocaust denial, and false pages promoting the Alternative für Deutschland party (AfD) party. In Italy, tactics included setting up general interest pages for beauty, football, health or other interests, then after followers signed up, transforming them into political tools (Graham-Harrison, 2019).

Telegram

Totally encrypted and largely unmonitored, the messaging application Telegram was created to provide a safe, uncensored communication platform. Launched in 2013, Telegram was not designed for engagement and amplification like Facebook, YouTube, and Twitter, but as a service for protecting free speech and facilitating communication against the backdrop of an authoritarian regime. Its founder and CEO, Pavel Durov, is sometimes called the Mark Zuckerberg of Russia. Unfortunately, while it counts hundreds of millions of users, the platform has grown most infamous as a safe-haven for extremists and terrorists. As Facebook and Twitter have cracked down more aggressively on hate speech over the recent year, Telegram became one of the new places where far-right groups found refuge. Telegram’s commitment to protecting freedom of speech above all else, undergirded by the app’s emphasis on strong encryption, has provided an attractive home for many of these extremists.

A Wired magazine report from March 2020 was entitled, “How Telegram became a safe haven for pro-terror Nazis” (Bedingfield, 2020). The report describes how Telegram is used by several dozen groups to disseminate white supremacist propaganda and videos of lynches and shootings. It also cites a new report from the political action group Hope not Hate that found that the platform is playing host to several dozen Nazi channels. These public and private chat groups, which post predominantly in English or Ukrainian are predominately US-based with a handful of UK groups, and dub themselves the “Terrorgram”. The groups are highly interconnected, often reposting content from each other’s channels. They draw influence from existing far-right terror groups like the Atomwaffen Division, the Nazi web forum Iron March, and the writings of American Neo-Nazi James Mason. The groups disseminate white supremacist propaganda, videos of lynches and shootings, survivalist and guerrilla training manuals, and instructions for manufacturing weapons, carrying out attacks and evading detection. The groups also canonize other famous terrorists as “saints”. Murderers who have received this designation include David Copeland, the 1999 London nail bomber, Anders Breivik, the perpetrator of the 2011 Utoya attack in Norway, and unexpected choices like the Islamist terrorist Omar Mateen.

Although Telegram has long been used by the far-right to communicate, there has been a noticeable surge in the number of channels and their users since the Christchurch massacre of March 15, 2019. The SITE Intelligence Group found that 80 per cent of a select sample of 374 farright Telegram channels and groups were created between the March 15 massacre and October 30, 2019 (Katz, 2019). The number of users in this community increased as well: a sample of far-right channels created in May 2019 collectively increased their memberships by 117 per cent – from 65,523 to 142,486 by the end of October. The biggest Terrogram groups have accrued over 4,000 followers in under a year. As Katz concludes, “Neo-Nazi and white nationalist groups now have in Telegram a centralized operational venue to network, recruit and distribute attack manuals, just as the Islamic State had for years”. Features such as media sharing, one-to-one chats and reposting from other channels and users are helping to weave the far-right’s various sub-movements together, building a unified umbrella of groups and ideologies.

Our survey of far-right content appearing on Telegram revealed a wide range of formats, from memes and cartoons to videos and images glorifying acts of violence. Some postings are digital libraries, intermingling white nationalist texts such as Mein Kampf and The Turner Diaries with detailed instructions on how to make homemade weapons or run a militia.

Dark Net

Think of the Internet as a huge iceberg. The tip of the iceberg, which most people can see, is the Surface Web that has been crawled and indexed and is thus searchable by standard search engines such as Google or Bing via a regular web browser. But most of the Internet lies below the metaphorical waterline, unsearchable and inaccessible to the general public. These hidden parts of the internet are known as the Deep Web. The Deep Web is approximately 400-500 times more massive than the Surface Web. The deepest layers of the Deep Web, a segment known as the Dark Net, contain content that has been intentionally concealed including illegal and anti-social information. The Dark Net can be defined as the portion of the Deep Web that can only be accessed through specialized browsers such as the Tor browser.

Terrorists and far-right groups have revealed the advantages of the Dark Net and started using their secretive platforms (Weimann, 2016b, 2016c; 2018). The uses of the far-right in the dark net are like the surface web. The key differences are in achieving anonymity and avoiding regulation and censorship. It is harder for authorities and social media companies to act against far-right activity on the dark web. Several surveys of dark net platforms revealed a rising presence of farright postings. Thus, for example, exploration and analysis of anti-Semitic activity on the dark web found a variety of white supremacist and Nazi-related items (Topor, 2019). For instance, Dream Market offered Hitler gold coins, Nazi-themed clothes, stamps, pictures, artwork, and so forth.

Far-right blogs on the dark web are another example of online racist propaganda and incitement. A typical example is a blog named White Will Survive, describing Jews as mentally ill, rapists, and having all the desire to kill everyone who is not Jewish. Searching the dark net for terms such as “Nazi,” “Jews,” “White,” and various other anti-Semitic and race-related terms yield troubling results. For example, these extremists frequently use the dark net blogs to post, discuss, disseminate and search for items like Holocaust denial and Nazi propaganda. Far-right groups also use social networks on the dark net. These are like surface web networks such as Facebook, Twitter, LinkedIn, Google+, or Gab. After restrictions and bans on these social networks in the surface web, many extremists moved to dark net social networks. The dark web has several popular social networks for far-right activists to thrive in, including a dark web version of Facebook. These versions provide the secrecy and anonymity that the surface web does not. Once inside a dark net social network, a variety of pages, users, and posts can be found. Many of these dark net social media are used to disseminate racist, white supremacist and anti-Semitic propaganda.

Capitalizing on the Corona Pandemic

The current coronavirus pandemic has brought an unprecedented threat to the lives, incomes, and well-being of entire populations. For far-right extremist groups, this is a unique opportunity to spread hate, fear, panic and chaos. As the virus spreads, it has become the most dominant content in far-right media and online chatter (Katz, 2020). Across far-right online platforms like Telegram and Gab and more conventional platforms like Instagram, Facebook and Twitter, far-right groups and individuals are promoting conspiracy theories, scapegoat refugees and advance the argument for closed borders. Other far-right extremists have gone further in advocating the use of the virus as a bioweapon against their enemies, asking individuals to willingly spread it. Since the outbreak in early December 2019, there have been posts on websites such as Telegram, 4chan and Gab linking the coronavirus to racist and anti-Semitic slurs and memes. This has ranged from racist posts to parodies of Chinese people mocking their hygiene and eating habits.

Among the far-right’s hate viruses are arrays of conspiracy theories. As Katz (2020) notes, these theories often play into anti-Semitism or xenophobia against people from China, pondering the role of the Chinese government or the “Jewish global elite” in the outbreak. As one typical posting argues, “This Jewish made coronavirus is affecting the international stock market...because our manufacturing is out sourced to thus is all relied upon by China...because of globalism; because of Jews.” A wide range of conspiracy theories are used including Jews are responsible for corona, Jews have been trying to spread it, Jews developed a vaccine that people should refuse to take, and that Jews are profiting off the disease. Other conspiracists advance the theory that the disease was manufactured by the US and or Israel as a biological weapon to target rivals such as China and Iran. This is not the first time this has happened. During the outbreak of the Black Death, Jews were used as scapegoats with accusations that the Jews had caused the disease by deliberately poisoning wells.

The most worrying aspect of the far-right’s coronavirus-related campaign is the call for actual attacks, suggesting that the current circumstances are both encouraging violence as well as helping attackers not get caught. Far-right terrorists have advocated using coronavirus as a bioweapon against their enemies: infected individuals should “visit your local synagogue and hug as many Jews as possible”, reads one post. One far-right poster similarly advises, “Cough on your local minority”. Another calls for the same tactics against critical infrastructure, writing, “Cough on your local transit system”. The Federal Protective Service (part of the Department of Homeland Security in the US) declared that “White Racially Motivated Violent Extremists have recently commented on the coronavirus stating that it is an ‘OBLIGATION’ to spread it should any of them contract the virus”.1 They added that they have specifically mentioned spreading the disease in public places and have used terms such as “corona-chan”, “bowlronavorus” (a reference to Dylann Roof) and “boogaflu” (modification of the term “boogaloo” used to reference a future civil war). In a Telegram group, they discussed options such as leaving “saliva on door handles” and spreading it amongst their “enemies”. Some far-right virus-related items include graphics like cartoons, posters, and pictures. One such graphic, falsely presented as being posted by the Center for Disease Control and Prevention (CDC), encourages people to visit mosques or synagogues and ride on public transit to refute public health and safety information and resources offered in those places.

Fake news, rumours, hoaxes, and conspiracy theories that have been spread during the Coronavirus crisis not only reify prejudices about Asians, Jews, Chinese, foreigners, immigrants but also present them in a causal structure. These are the causes for the virus, they are to be blamed and punished. The politicization of Coronavirus by the far-right points to how these modes of discourse serve as narratives that reinforce racist and anti-Semitic concepts and beliefs.

Finally, a crisis like the Coronavirus pandemic, when people are panic-driven consumers of news, is ideal for suppliers of fear, hate and lies. The far-right is capitalizing on the occasion, flooding online platforms, in surface net and dark net formats, with apocalyptic narratives, whether of societal collapse or race war. These narratives use the rising fear to attract interest, draw followers closer, and spread the extremists' theories and perception. This is the toxic virus of the far-right, seizing the opportunity to promote their narratives to scapegoat groups like immigrants, or minorities, or liberals.

#### That ensures large-scale bioweapon attacks – the far right has unique access to materials and know-how.

Daniel Koehler and Peter Popella 17. Fellow at George Washington University’s Program on Extremism, Editorial Board Member of the International Centre for Counter-Terrorism (ICCT) in The Hague and Founding Director of the German Institute on Radicalization and De-Radicalization Studies (GIRDS). Scholar of microbiology and specialist for infectious bacteria and antibiotic resistances, holds a B.Sc., M.Sc. and Ph.D. degree from the Eberhard Karls University Tuebingen, Germany. “BEWARE OF CBRN TERRORISM FROM THE FAR-RIGHT”. Small Wars Journal. Sept 19 2017. https://smallwarsjournal.com/jrnl/art/beware-of-cbrn-terrorism-from-the-far-right

As the threat from domestic terrorism is clearly increasing, one must ask if violent tactics used by these attackers might develop beyond the use of explosives and guns. The vehicle attack in Charlottesville was an indication of that tactics diversification, even though this was not the first incident of its kind in the United States. As the Oklahoma plot shows, far-right terrorists might see themselves in some kind of competition for public recognition with Jihadist groups like ISIS, which could lead to a further escalation of tactics used for example with the deployment of chemical, biological, radiological or nuclear (CBRN) weapons. In fact, right-wing terrorists have for decades been attempting to develop and use chemical and biological weapons. This article aims to give a short overview on the history of such efforts, the potential for right-wing terrorism to use chemical and biological agents in the future, and how authorities can counter this threat.

A Look at the Cases

Even though no significant cases of successful right-wing CBRN terror attacks in Western countries are known, a number of plots have been uncovered that indicate the motives and tactics of these extremists. In 2009 Ian Davidson, who was the leader of the right-wing terrorist Aryan Strike Force (ASF), became the first British citizen convicted of producing a chemical weapon of mass destruction. When Davidson and his son Nicky were arrested in the United Kingdom, the subsequent trial and conviction made history. His plot aimed to poison water supplies of Muslims in Serbia using the toxin ricin, which he already had produced in a significant amount. Estimations by investigators regarding the lethality of the material varied drastically but some thought the amount produced by Davison could have killed up to 1,000 people.

In the mid-1980s one of the few right-wing terrorist organizations in the United States, “The Covenant, the Sword, and the Arm of the Lord”, acquired large amounts of cyanide, intending to poison water supplies in major U.S. cities, but failed to overcome the technical difficulties of dissemination. In May 1996, a laboratory staff member and white supremacist in Ohio, Larry Wayne Harris, successfully acquired plague bacteria – not illegal at that time. Two years later, Harris and a co-conspirator were arrested for threatening to release anthrax in Las Vegas, even though his strain was a vaccine grade and harmless version. Material to extract ricin was also found at the home of white supremacist James Kenneth Gluck in Tampa, Fla., who was arrested by the FBI in November 1999 after he threatened judges with biological warfare. More serious seems to have been the plot led by neo-Nazi William Krar of Texas, arrested in April 2003. Investigators found more than 500,000 rounds of ammunition, 65 pipe bombs and remote-control briefcase bombs, and almost two pounds of deadly sodium cyanide. Along with white supremacist and anti-government material, components to convert the cyanide into a bomb capable of killing thousands were also secured. In November 2011, a plot to blow up government buildings and kill masses of people using ricin by a group of four men belonging to an anti-government militia in Georgia was uncovered. Especially concerning was the fact that one of the four was working for the federal Department of Agriculture, giving him access to chemicals, technical equipment and ways to disseminate the poison into food and water supplies. In February 2017, 27 year old William Christopher Gibbs, member of the white supremacist Creativity Movement, was arrested after hospitalizing himself for side effects of his experiments with ricin, triggering a large FBI operation.

When looking at these cases, far-right extremists attempting to acquire and use CBRN weapons have very mixed backgrounds, ranging from career criminals to senior biodefense researchers at United States Army institutions. However, the more serious plots came from well-educated individuals with necessary access to equipment and dissemination ways indicating that right-wing terrorists might be quite well embedded in Western societies. In his seminal study about far-right terrorists’ recruitment and radicalization from 2012 for example, Pete Simi found 56% of his sample belonged to middle or upper social class and 53% had some form of college or higher education (with and without degrees). The majority of far-right CBRN plotters were part of groups and networks associated with their ideological and criminal conduct but not all of them. However, every far-right CBRN incident appears to be a culmination of a radicalization escalation process, sometimes even over years, with long histories of openly expressed violent, right-wing extremist, racist or anti-government opinions. Many of the plotters repeatedly threatened to use CBRN weapons in public to bystanders, families or friends. Even the lone actors were known to have gradually distanced themselves from their social environments getting more and more agitated and aggressive.

Now, the key question is: what makes a threat of far-right CBRN terrorism more likely and dangerous than compared with other violent ideologies, such as left-wing or jihadi terrorism? Of course, far-right extremists have equal access to open market technical equipment and supplies for manufacturing such weaponry as all other extremists in the country and their ideology is not more or less dangerous than jihadi or left-wing extremism, for example. Nevertheless, in 2012 international terrorism expert Peter Bergen stated, that “11 right-wing and left-wing extremists have managed to acquire CBRN material that they planned to use against the public, government employees or both” while there was no evidence of jihadists in the United States managing to do that. From these 11 cases only one (Joseph Konopka) was motivated by left-wing extremist (more specifically anarchist) political ideals. This fact is striking, since other violent extremists, especially Jihadists, certainly do not lack the willingness to use weapons of mass destruction (WMDs), as it is currently experienced in Syria and Iraq. But how indicative is this retrospectively almost singular right-wing CBRN terror threat for the future?

To assess the possibility of an attack, one has to take three factors into account: 1) the feasibility of the used weapon (acquisition, available know-how, technology, materials or agents), 2) the “effectivity” or costs and benefits of the weapon and 3) the motivation to use the weapon regarding the pursued aims. The assassination of an individual person with a plain firearm is feasible (through the ease of acquiring a firearm), effective (since a single, well-placed bullet will “do the job”) and sends a clear message in terms of motivation, however not to an extent exceeding every-day criminality encountered on the streets of big cities. Using a deadly toxin, like ricin, presents bigger hurdles in terms of feasibility, but is also highly effective (in terms of toxicity and evasion of forensic investigation) and, more important, will provide added value in terms of public attention and media coverage about the attack and the very ideology of the originators. Considering the attack on a crowded public space, planting explosives will lead to severe damage as well potentially high lethality. However, by mixing the explosives with radioactive material – a so called dirty bomb – will not only cause more fatalities through radiation, but also evoke a higher level of fear and terror. Additionally, such an incident would represent a difficult challenge for first responders and might render the government incompetent of an appropriate response and preparation in the eyes of the public. All terrorists potentially share this goal to make their attacks more impactful and deadly, even though right-wing terrorists rarely have aimed to produce mass casualties, so far.

Factor 2, the effectivity of a weapon is, depending on the planned operation, similar for all kinds of terrorist as well. However, the feasibility to use CBRN weapons (factor 1) might be higher for far-right terrorists than for others, e.g. jihadists, since the extreme right can rely on established and much larger support networks, which can provide the required material, know-how and dissemination ways. Of course, it is not impossible for lone actors from all ideological strands to acquire the material as well as the know-how. Regarding factor 3, the motive, the violent far-right might be in an extraordinary position right now, making it more dangerous than ever.

The current Trump administration is openly courting the extreme right and – in the eyes of observers – fuelling a rising far-right terror threat, for example through the inadequate reaction to the Charlottesville attack. In addition, the general public is much less likely to perceive violent actions from far-right extremists as “terrorism” compared, for example, with those acts by Islamic extremists. This gives violent extremists from the far-right considerably more space to radicalize, escalate violent tactics and plot attacks without interference from the outside than from any other violent extremist group in Western countries. The most significant danger, however, will come to light after the demise of the Trump administration. A future US government trying to put the far-right jinni that Trump has released back into the bottle will face a much stronger, self-confident and aggressive opponent, already dreaming of a race war. The current government is favoured by anti-government militias and sovereign citizens and they are looking for a new enemy: those “counter-revolutionaries” attempting to return the United States to a pre-Trump state. Even open civil war was threatened in a case of impeachment. far-right extremists of all different strands might have heavily stockpiled firearms and explosives, but they know they cannot outgun and outman law enforcement, National Guard or the Military. A fight to retain their perceived newly gained freedom and powers therefore must include a tactical edge forcing the government to refrain from a too aggressive crackdown. CBRN agents or even the potential to quickly acquire them are the most effective and logical way to ensure the government’s passivity, especially giving the history of CBRN plots within the far-right.

What is Likely, What is Not? A Choice of Weapons

Some CBRN agents are more likely to be used in a terrorist attack than others, depending on factors such as ease of acquiring raw materials, difficulty of production, the required know-how, danger of storing the material for the terrorist, degradation of the material over time, deliverance, dispersion, and potential countermeasures. Nuclear and radiological weapons require radioactive elements that are generally stored under high-security and thus hard to obtain without a state sponsor. Low-level radioactive elements unsuitable for nuclear weapons, but sufficient for the construction of a ‘dirty bomb’ might be easier to obtain, since industry, agriculture and medical institutions are dependent on them. Americium, which is used in household smoke detectors, has indeed been found in the homes of far-right extremists, e.g. Tampa resident Brandon Russell. However, its actual effectiveness as a dirty-bomb ingredient is debated. Further, neo-Nazi James Cummings acquired four 1-gallon containers with a radioactive uranium and thorium mix in 2008, along with highly toxic beryllium powder and instructions to build a dirty bomb.

Chemicals and biological material, while for some part underlying governmental restrictions concerning proliferation and acquisition, are much easier to access. As noted by Edward You of the FBI’s Weapons of Mass Destruction Directorate, Biological Countermeasures Unit, “The materials are readily available (…), and the majority of equipment can be purchased outright and do not fall under any regulatory regime.” Precursors for chemical warfare agents, as sodium cyanide in the case of William Krar, can be simply bought online. Manuals explaining the synthesis of the active agents in small laboratory or kitchen setups have been found in many cases, illustrating that the required knowledge has already spread and advanced significantly. Explosives that have been found and used in terror associated cases include the so called ‘mother of Satan’, triacetone peroxide (TATP), and hexamethylene triperoxide diamine (HTMD). TATP can be synthesized from easily accessible household chemicals (acetone, hydrogen peroxide and sulfuric acid). Synthesis of chemical warfare agents like sarin, a nerve agent used by the Aum Shinrikyo attacks on the Tokyo subway, is highly demanding in terms of technology and know-how. Considering the difficulties of achieving sufficient quality of the material and the high risk for the producers during manufacturing and storage make and attack with nerve agents appear unlikely. However, structurally more simple chemicals, like cyanide compounds which can be commercially obtained, have been used in far-right terror plots.

Another potential dual-use chemical is chlorine. The highly reactive gas is nowadays widely used as disinfectant, bleaching agent and within different industry branches. Millions of tons are transported on roads and railways within the US every year, and may as such be targets for terrorist attacks. Upon contact with the human mucosa, the water soluble chlorine will at first cause local irritations and, during prolonged exposition of higher doses, evoke the deadly “dry-land drowning”. While no large scale attacks on hazardous material (HAZMAT) transports have been reported so far, guides to derail trains carrying such materials have been published by Jihadists and could easily be used by far-right terrorists as well. Additionally, application of commercially acquired chlorine as choking agent in local, small scale attacks pose a risk.

Alternatives to chemicals are agents of biological origin: toxins, bacteria (or spores – robust and dormant forms) and viruses. Toxins are harmful products of biological organisms, which interfere with vital body functions. Production and purification of these substances require in-depth knowledge and large amounts are thus hard to obtain. Ricin, which can be isolated from the castor oil plant, has been detected in multiple cases of far-right terror plots. While ricin is extremely deadly when taken up into the body, a wide spread application of ricin to target large groups of people is rather unlikely, just by the large amounts needed for such operation and the very proteinaceous nature. The isolation and cultivation of bacteria, although requiring some microbiological knowledge, can be done in improvised laboratory setups. Highly pathogenic strains are usually kept in isolated, high-security laboratories. However, Bacillus anthracis is an omnipresent, easy to isolate soil bacterium. Anthrax, as in the case of Larry Wayne Harris, is according to the CDC generally considered to be the most likely agent which might be used in large-scale bioterror. Viruses are dependent on cells as hosts for multiplication and thus require an even more complicated production process, which is highly unlikely to be established outside of academic or industrial laboratories. While the deadliest infectious diseases, like ebola or lassa, are caused by viral infections, application of viruses as terror agent by far-right extremist is unlikely. However, the growing industry and professionalization of DIY bio-laboratories across the United States was also noted by the FBI, which might also increase accessibility of the necessary technical equipment for potential biological and chemical terrorism.

Likely Goals of Right-Wing Terrorists

Existing research on right-wing CBRN terrorism is scarce and outdated. Few experts have even considered the potential threat, mostly in the late 1990s looking at Christian Millenarianism as a form of religious terrorism aiming for the apocalypse in a “sacrificial ritual of mass murder and suicide ”. Even though Christian millenarian groups have not attempted to develop CBRN weapons, they were scrutinized for such a potential threat after the Aum attack in Tokyo. Jessica Stern wrote in 1999 that “the costs of escalation to biological weapons seem to outweigh the benefits” for domestic extremists. Paul Blister and Nina Kollars confirmed this notion regarding the Christian Patriot Movement in 2011. Right-wing terrorism, however, goes beyond Christian fundamentalism and fanaticism circling around Armageddon. Especially given the dramatic increase in anti-government sentiment and militia groups in some western countries (e.g. the US and Germany) and their partial overlap with white supremacist and nationalist groups, there is potential for a future escalation of violent tactics if anyone might attempt to contain them again. Right-wing terrorists have usually not sought large public audiences for their attacks in order to communicate specific political programs but rather to annihilate their enemies by every means possible. In addition, to create chaos and panic, as well as erode a public’s trust in the government’s ability to provide safety by demonstrating its helplessness – a concept known as ‘strategy of tension’ among right-wing extremists – is thought to break the government’s monopoly of force and core political legitimacy.

Other research about right-wing extremism and terrorism has also shown, that an overlap between violent activists from the far-right and organized crime exists, which means that the acquisition of WMDs by these groups and actors could also be used as significant tool to shift the power base in extortion operations towards what could become right-wing extremist crime syndicates. In Austria for example a neo-Nazi group called ‘Object 21’ controlled large parts of the red light milieu along the Austrian-German border through the use of explosives, arson and attacks with butyric acid. In the United States, neo-Nazi oriented networks such as the Aryan Brotherhood for example, are deeply involved in drug trafficking. Highly militant and criminal hybrid networks could have severe impact within the organized crime world if they get their hands on CBRN weaponry, which is of course true not only of far-right but also for other terrorists.

#### Extinction!

Owen Cotton-Barratt et al. 17. PhD in Pure Mathematics from Oxford, Lecturer in Mathematics at Oxford, Research Associate at the Future of Humanity Institute; Sebastian Farquhar, PhD student in Computer Science at Oxford; John Halstead, DPhil in Political Philosophy from Oxford, former Research Fellow at the Global Priorities Project; Stefan Schubert, Ph.D. in philosophy from Lund University, former postdoc at London School of Economics; Haydn Belfield, Academic Project Manager at the Centre for the Study of Existential Risk, BA in PPE from Oxford; Andrew Snyder-Beattie, leads Open Philanthropy's work on biosecurity and pandemic preparedness, former Director of Research at the Future of Humanity Institute, PhD/DPhil in Zoology from the University of Oxford. “Existential Risk: Diplomacy and Governance”. pg. 9. GLOBAL PRIORITIES PROJECT 2017. <https://www.fhi.ox.ac.uk/wp-content/uploads/Existential-Risks-2017-01-23.pdf>

1.1.3 Engineered pandemics

For most of human history, natural pandemics have posed the greatest risk of mass global fatalities.37 However, there are some reasons to believe that natural pandemics are very unlikely to cause human extinction. Analysis of the International Union for Conservation of Nature (IUCN) red list database has shown that of the 833 recorded plant and animal species extinctions known to have occurred since 1500, less than 4% (31 species) were ascribed to infectious disease.38 None of the mammals and amphibians on this list were globally dispersed, and other factors aside from infectious disease also contributed to their extinction. It therefore seems that our own species, which is very numerous, globally dispersed, and capable of a rational response to problems, is very unlikely to be killed off by a natural pandemic.

One underlying explanation for this is that highly lethal pathogens can kill their hosts before they have a chance to spread, so there is a selective pressure for pathogens not to be highly lethal. Therefore, pathogens are likely to co-evolve with their hosts rather than kill all possible hosts.39

Recent developments in biotechnology may, however, give people the capability to design pathogens which overcome this trade-off. Some gain-of-function research has demonstrated the feasibility of altering pathogens to create strains with dangerous new features, such as vaccine-resistant smallpox40 and human-transmissible avian flu,41 with the potential to kill millions or even billions of people. For an engineered pathogen to derail humanity’s long-term future, it would probably have to have extremely high fatality rates or destroy reproductive capability (so that it killed or prevented reproduction by all or nearly all of its victims), be extremely infectious (so that it had global reach), and have delayed onset of symptoms (so that we would fail to notice the problem and mount a response in time).42 Making such a pathogen would be close to impossible at present. However, the cost of the technology is falling rapidly,43 and adequate expertise and modern laboratories are becoming more available. Consequently, states and perhaps even terrorist groups could eventually gain the capacity to create pathogens which could deliberately or accidentally cause an existential catastrophe.

# 2ac – texas r1

## platforms adv

### innovation turn – 2ac

#### Small firms – interoperability allows them to piggyback off of existing innovations. Current failures are because starting from the ground up is impossible. That’s Sharma, AND...

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

Competitive compatibility means that competitors can interoperate with bigger services and platforms without having to negotiate with them, ask their permission, or risk breaking a number of computer crime and intellectual property laws. Interoperability mandates go further to make that interoperability usable, stable, and accessible for users: data portability would make it easy for users to move from one platform to another; back-end interoperability would create the infrastructure for users from one platform to interact with users on another; and delegability would give users the ability to delegate an external tool to interact with a platform for them.

3.1. Competitive Compatibility

We support a legal regime that will unlock and encourage competitive compatibility (ComCom): the ability of a competitor to interoperate with an incumbent’s products or services without permission.

ComCom is absolutely essential for innovation. Overwhelmingly, the technologies we rely on today were not established as full-blown, standalone products; rather, they started as adjuncts to the incumbent technologies that they eventually grew to eclipse. The first cable TV service grew out of hobbyist efforts to bring big-city TV networks to their small-market towns. Modems were unsanctioned add-ons to Ma Bell’s ubiquitous copper phone lines. Before the Web, a tool called Gopher defied network operators’ intentions and made information from around the Internet accessible to the masses. Printers, ad-blockers, tape-deck audio jacks, and personal finance empires grew and thrived—not because anyone deliberately let them, but because nobody could stop them.

We propose that users and companies should have the right to build around, and on top of, incumbent tools and services. Start-ups should have the right to engage with users on their competitors’ platforms, to chip away at the network effects that would keep them down. Users should have the right to engage with the platforms they use in any way they want, including through third-party tools that tune their experience. Nobody should receive a cease-and-desist for sharing a browser extension to improve a product they spend all day using.

#### Big firms – diversified platform marketplace forces them to innovate to keep consumers. That’s Schulman, AND...

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. “Unfair Use: Anti-Interoperability and Our Dwindling Digital Freedom”. The Reboot. Apr 13 2021. <https://thereboot.com/unfair-use-anti-interoperability-and-our-dwindling-digital-freedom/>

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.

## middleware adv

### AT: bubbles – 2ac

#### Status quo doesn’t solve/counterplan unconstitutional – removing far-right content’s impossible. Try-or-die to limit its reach.

Francis Fukuyama 21. Mosbacher Director of Stanford’s Center on Democracy, Development and the Rule of Law. Director of the Ford Dorsey Master's in International Policy at Stanford. PhD, political science, Harvard. “Making the Internet Safe for Democracy”. Journal of Democracy, Volume 32, Number 2, April 2021, pp. 37-44. <https://muse.jhu.edu/article/787834/pdf?casa_token=VdaYtO26fNMAAAAA:aM5-x7m0oZADeR-FmoDEVkwwyKzCw2-uzMpN3dxf92QDv6FDYmwObGP6bze5Rmd_lsg5XiFkN3t_>

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.

## expand the scope

### nu exemptions – 2ac

#### 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 determined by adjudication.

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.

This uncertainty surrounding the scope of Section 5 is exacerbated by the administrative procedures available to the Commission. Consider the following empirical observation. The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges in the past nearly twenty years. In each of those cases, after the administrative decision is appealed to the Commission, the Commission has ruled in favor of FTC staff and found liability. In other words, in 100 percent of cases where the administrative law judge ruled in favor of the FTC staff, the Commission affirmed liability; and in 100 percent of the cases in which the administrative law judge ruled found no liability, the Commission reversed.2 This is a strong sign of an unhealthy and biased institutional process. By way of contrast, when the antitrust decisions of federal district court judges are appealed to the federal courts of appeal, plaintiffs do not come anywhere close to a 100 percent success rate—indeed, the win rate is much closer to 50 percent. Even bank robbery prosecutions have less predictable outcomes than administrative adjudication at the FTC. One interpretation of these historical data is that the process at the FTC stacks the deck against the parties. Another is that the FTC has an uncanny knack for picking cases; a knack unseen heretofore within any legal institution. I will allow discerning readers to choose the most likely of these interpretations—but suffice it to say the “case selection” theory requires one to also grapple with the fact that Commission decisions, when appealed, are reversed at a rate four times greater than antitrust opinions by generalist federal judges.3

Significantly, the combination of institutional and procedural advantages with the vague nature of the Commission’s Section 5 authority gives the agency the ability, in some cases, to elicit a settlement even though the conduct in question very likely may not be anticompetitive. This is because firms typically will prefer to settle a Section 5 claim rather than to go through lengthy and costly litigation in which they are both shooting at a moving target and have the chips stacked against them. Such settlements also perpetuate the uncertainty that exists as a result of the ambiguity associated with the agency’s “unfair methods of competition” authority by encouraging a process by which the contours of Section 5 are drawn through settlements without any meaningful adversarial proceeding or substantive analysis of the Commission’s authority.

The second principal reason Section 5 has failed to contribute effectively to the Commission’s competition mission is because of the absence of even a minimal level of certainty for businesses. A stable definition of what constitutes an “unfair method of competition” would provide businesses with important guidance about what conduct is lawful and what conduct is unlawful under Section 5. The benefit of added business certainty is less important than ensuring Section 5 enforcement actions—including consents—actually reach and deter anticompetitive conduct rather than chill procompetitive conduct. However, guidance to the business community surely is important. Indeed, the FTC has issued nearly 50 sets of guidelines on a variety of topics, many of them much less important than Section 5, to help businesses understand how the Commission applies the law and to allow practitioners to better advise their clients on how to comply with their legal obligations. Without a stable definition of what constitutes an “unfair method of competition,” businesses must make difficult decisions about whether the conduct they wish to engage in will trigger an investigation or worse. Such uncertainty inevitably results in the chilling of some legitimate business conduct that would otherwise have enhanced consumer welfare but for the firm’s fear that the Commission might intervene and the attendant consequences of that intervention. Those fears would be of little consequence if the agency’s authority was defined and businesses could plan their affairs to steer clear of its boundaries.

Some commentators have asserted that formal agency guidance would too severely restrict the Commission’s enforcement mission.4 They warn that defining the boundaries of the Commission’s “unfair methods of competition” authority would achieve stability and clarity only at the expense of creating an enforcement regime that fails to adequately protection competition. These commentators instead urge reliance upon the same case-by-case approach that has garnered success in the context of the traditional antitrust law. Under this view, the scope of the Commission’s authority to prosecute unfair methods of competition is best determined by reading the leading cases to identify which enforcement principles the Commission applies when determining whether to prosecute a particular business practice under Section 5.

#### 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?

## regulation cp

### regulate – 2ac

#### 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 Sharma. 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 vagueness 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.

#### FTC avoids it.

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.

3. Regulatory Capture

Finally, it is worth noting that the FTC is in far less danger than the DOT of being "captured." Capture is a widely studied phenomenon in which a regulator aligns its interest with the industry it regulates. 149 Capture is more likely when a regulator faces only one industry, like DOT's aviation consumer protection division. 150 The FTC, on the other hand, does not have a constituency. Its general enforcement mandate is spread over multiple industries, meaning that there is little repeat play. 151

## populism da

### populism – 2ac

#### Khan.

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.

#### The public is demanding antitrust reform. Failure to cave ensures social unrest, collapse of democratic legitimacy, and overregulation.

Ariel Katz 20, Associate Professor of Law at the University of Toronto, 2020, “The Chicago School and the Forgotten Political Dimension of Antitrust Law,” University of Chicago Law Review, Vol. 87, Issue 2, Article 6, <https://chicagounbound.uchicago.edu/uclrev/vol87/iss2/6>

Moreover, in a democracy, the success of the antitrust enterprise depends on the public’s continuing support. But, as Daniel Crane noted recently:

The bipartisan consensus that antitrust should solely focus on economic efficiency and consumer welfare has quite suddenly come under attack from prominent voices [from the political left and right] calling for a dramatically enhanced role for antitrust law in mediating a variety of social, economic, and political friction points, including employment, wealth inequality, data privacy and security, and democratic values.164

Crane also describes how “the rising tide of calls for a radically different version of antitrust has led to a circling of [the bipartisan antitrust] establishment wagons around the consumer-welfare standard” despite major disagreements within this establishment on the meaning and implementation of that standard.165

Such a response by the establishment may not be the most productive. If dissatisfaction with the current antitrust status quo becomes a shared view of the political left and the right in a period when they seem incapable of finding common ground on almost any issue, then insisting that the status quo is just fine and that the criticism is based on fundamental misunderstanding of existing antitrust’s greatness may not be very persuasive. Put differently, if growing swaths of the public become concerned about the distribution of power and its exercise, then telling them that antitrust should only care about efficiency may cause them to abandon their support for the antitrust enterprise altogether.

Furthermore, there may be other costs to ignoring antitrust’s political dimension. One of the motivations for adopting the antitrust laws (and the reasons why the antitrust enterprise also gained the support of business) was the realization that the ills of monopoly, not only high prices, but also the helplessness of those who have little choice but to depend on the monopoly, may lead to social unrest. In the worst case, this might lead to a loss of credibility for democratic governance and even to the rise of totalitarianism, or at least to excessive intervention of the government in the operation of markets, either by way of overregulation or central planning. Thus, the alternative to vigorously enforced competition laws is not the classic economist’s liberal laissez-faire utopia, but a society that is neither free nor productive.

To the extent that the present crisis of liberal democracy and the rise of illiberal tendencies in many countries is connected, at least in part, to the reign of Chicago School economics (and other neoliberal prescriptions) and the frustration of those who found themselves waiting in vain for economic benefits to trickle down, then insisting on a business-as-usual approach to antitrust law and policy may come with a high price. In other words, however skeptical one might be about the desirability of acknowledging antitrust’s political dimension, the alternative—ignoring it— might be worse.

#### No impact to populism – political incompetence, safety valves

Moravcsik, PhD, 20

(Andrew, Politics@Princeton, https://foreignpolicy.com/2020/09/24/euroskeptic-europe-covid-19-trump-russia-migration/)

Over the past two decades, extreme-right populist parties with anti-Muslim, anti-immigrant, anti-terrorist, and anti-Europe appeal have increased their vote shares across Europe. They now participate in government in six countries. In Britain, they spearheaded Brexit. And in the last two decades, scholars—and, it seems, journalists—have written more about extreme-right populist parties than all other European parties combined. Leading foreign-policy pundits argue that homegrown extremism in Europe, the United States, and elsewhere—and not rising great-power challengers—now poses the greatest threat to the post-Cold War liberal international order. In Europe, many fear that extremist governments might win more EU exit referendums or join Trump and Putin in adopting protectionist and pro-Russia stances. Yet this proved to be journalistic hype. Rather than panicking over populist threats, European leaders calmly drained their energy by dampening migration and terrorism and hanging tough in negotiations with Britain—to which they can now add the political benefit of managing the coronavirus pandemic well. Today, European unity—in any case, a practical necessity for small and highly interdependent states—is more popular than at any time in recent history. In fact, populists were never as powerful as headlines made them seem. Consider the case of Marine Le Pen, who heads the French extreme-right National Rally party. When she ran for the French presidency in 2017, newspapers across the globe proclaimed, as one New York Times article put it, that “the next president of France will be Marine Le Pen” and speculated what her administration would do once in office. Yet her campaign was clearly hopeless from the start. All of her potential rivals, polls showed, could defeat her by comfortable double-digit margins, and Emmanuel Macron eventually did so by winning twice as many votes. Today, the National Rally holds just seven of 577 seats in the National Assembly. Outside of Britain, extreme Euroskepticism enjoys scant support. The impotence of the extreme-right in France is no exception. Outside of Britain, extreme Euroskepticism enjoys scant support. Of 27 EU members (plus Britain), 12 have no extreme-right or Euroskeptic party at all or none that scores above 10 percent in national elections. In 10 more countries, including France and Germany, other parties consistently exclude extremists from government coalitions. In three more—Latvia, Estonia, and Bulgaria—extremists participate only as minority coalition partners, which reduces their influence close to zero. Only in Britain, Hungary, and Poland does an extreme-right or Euroskeptic party actually lead the government. Of course, their extremism poses threats to the quality of democracy and rule of law, as in the United States, but their effect on foreign policy is slight. Migration is the only EU issue on which policy has moved in a direction extremists favor—but this, as we have seen, is only because the position held by extremists happens to be that of large majorities of moderate voters in nearly every country. Otherwise, Poland and Hungary, both of which are among the biggest beneficiaries of EU policies and have exceptionally pro-EU populations, follow their neighbors on nearly every aspect of external policy, from sanctions on Russia to development aid to Africa—dissenting occasionally only on symbolic declarations. That leaves Brexit as the only major Euroskeptic achievement of a populist party in recent years. Yet Brexit is, at best, an exception that proves the rule. That it happened at all reflects a perfect storm of astonishingly unlikely circumstances unrepeatable elsewhere. Britain is the only European country where Euroskepticism attracts more than a tiny fringe of the electorate. Even so, Brexit could happen only because a prime minister overruled his advisors to call an unnecessary referendum, which happened to fall at the only brief moment in the last five years when a majority of Britons opposed EU membership. Brexit was later ratified by an election in which a 44 percent vote share gave Boris Johnson a comfortable majority: Without Britain’s electoral institutions, the most biased in Europe, a pro-EU majority would have ruled instead. Today, Brexit remains stalled. Britain is much smaller and dependent on Europe’s good will to gain access for nearly half of its exports, particularly of services like banking. This allows Europe to take a tough stance in negotiations over the terms of the U.K. withdrawal. British Brexiteers once hoped that Trump would bail them out with a quick trade agreement. Yet U.S.-U.K. negotiations have gone nowhere after the United States badgered the British about agricultural imports and aircraft subsidies. Trump embarrasses prime ministers on his visits, remains unpopular among the British public, and is struggling to be reelected. Britain is running out of options. These realities, combined with the more general lack of support for their Euroskeptic views, have led populists elsewhere to moderate their ideas rather than follow London’s lead. Five years ago, 15 extreme-right parties, including Le Pen’s National Rally, advocated a Brexit-style withdrawal from the EU or the eurozone. Today none do. Even so, the most worrisome populist challenger in Europe, Matteo Salvini of the League party, is hemorrhaging popular support to the Brothers of Italy, a new and less Euroskeptic right-wing party. The wave of populist Euroskepticism seems to have crested.

#### Populism won’t cause great power war

Cooper 16 [Louis F. Cooper, His online writing includes “Reflections on U.S. Foreign Policy” at the U.S. Intellectual History Blog (July 16, 2014). His Ph.D. is from the School of International Service, American University., 12-6-2016, "WPTPN: Will Populist Nationalism Lead to Great-Power War?," No Publication, http://duckofminerva.com/2016/12/wptpn-will-populist-nationalism-lead-to-great-power-war.html]

Several reasons present themselves. First, nuclear weapons have given the prospect of a global war, or any great-power war, a possibility of civilization-ending finality that it did not have in the past. Second, the security architecture created under U.S. leadership after World War II has arguably worked to reduce the likelihood of major armed conflict among the great powers. Third, the existence of a network of international institutions, both inside and outside the UN system, has pushed in the same direction. Fourth, it is very possible that, as John Mueller and Christopher Fettweis have argued, decision-makers have to come see great-power war as “subrationally unthinkable, or not even part of the option set for the great powers.”[ii] The extreme destructiveness of the twentieth century’s world wars, fueled partly by developments in technology, might well have produced long-term effects on how leaders and publics think about global or great-power war, in a way, for instance, that the Napoleonic Wars, for all their horror and bloodiness, did not. Phil Arena’s recent contribution to this series argues that if the U.S. under a Trump administration signals an unwillingness to defend its allies, then Putin might be tempted to gamble on an invasion of the Baltics or Kim Jong-Un similarly might gamble on an invasion of South Korea (and that would drag in China). Putting aside Kim Jong-Un for the moment as a special case, let’s consider Putin. As long as NATO exists – and Trump, despite his statements about the unfairness of the distribution of cost burdens, has not suggested, as far as I’m aware, that he wants to dissolve the alliance – then Putin would have to assume that an attack on the Baltics would trigger a NATO response. Even if Putin does not see great-power war as unthinkable or outside his “option set,” one would assume that for reasons of pure self-interest he would not want to risk a nuclear war. Nor, one might think, would he want to jeopardize the prospect of better (from his standpoint) relations with a U.S. administration less concerned with, among other things, his commission of war crimes in Syria or his annexation of Crimea than the Obama administration has been. For these reasons, I’m not too worried that the advent of the Trump administration will lead to a war with Russia over the Baltics. The Korean peninsula is, perhaps, a more worrisome situation. Chances are, however, that Trump, after taking office, will be prevailed upon to make reassuring noises about the U.S. commitment to South Korea, and that should suffice to deter Kim Jong-Un from doing anything too rash. The cautionary point here, admittedly, is that it’s not clear whether Kim can be counted on to behave in a minimally rational fashion. Putin, whatever one might think of him, is rational. It’s not entirely clear whether Kim is. However, if Kim is irrational then all bets are off regardless of what U.S. policy pronouncements are forthcoming. World politics is not invariably cyclical and states can learn from experience (as even Gilpin acknowledged). If one admits this and pays due attention to history, then it is plausible to think that the force of populist nationalism, as expressed in more erratic and/or less ‘internationalist’ official policy, will not, whatever its other effects may be, increase the low likelihood of a global war.

## ftc da

### ftc privacy da – 2ac

#### Link thumper from other page. AND, no link – clarity – aff sets clear, certain norms for industry without litigation costs. That’s Sharma, AND...

Royce Zeisler 14. J.D. Candidate, Columbia Law School; B.S., B.A. 2012, University of British Columbia. “CHEVRON DEFERENCE AND THE FTC: HOW AND WHY THE FTC SHOULD USE CHEVRON TO IMPROVE ANTITRUST ENFORCEMENT”. 2014 COLUM. BUS. L. REV. 266. 2014. Lexis.

Importantly, the FTC Act not only created a new category of antitrust liability, but it also created a new norm-creator for defining that category: the FTC itself. That is, through the administrative structure of the FTC, Congress made clear that the FTC should be a dynamic norm-creator. Specifically, Congress paralleled the novel agency framework of the Interstate Commerce Commission ("ICC") and established the FTC as an independent agency that could bring cases through internal adjudication and issue cease-and-desist orders. 27 This structure meant and continues to mean (1) that section 5 cases do not go before juries, 28 (2) that Article III appellate courts use the FTC's administrative record, and (3) that the FTC's factual conclusions are reviewed under the substantial evidence standard. 29 Thus, [\*274] much like the Sherman Act, section 5 was intended to be flexible and evolve as business practices changed. 30 Unlike the Sherman Act, however, Congress did not leave this development solely to the judiciary.

The differences between the Clayton and FTC Acts reinforce that Congress intended the interpretation of section 5 to be independent of other antitrust terms. Under the Clayton Act, Congress granted the FTC enforcement, but not norm-creating, powers. Congress granted standing to the FTC, DOJ, ICC, Federal Reserve Board, and private citizens to enforce various sections of the Clayton Act involving mergers, 31 exclusive dealing, 32 and price discrimination. 33 Along with these multiple enforcers came a collateral estoppel provision. This provision explicitly gave private plaintiffs the right to use government litigation as preclusive (and gain treble damages). 34 In contrast, section 5 enforcement actions have no collateral effect on other litigation, and no other actors have standing to enforce it. 35 [\*275] Thus, while the Clayton and Sherman Acts created liability provisions that allow for multiple enforcers, section 5 created a unique area of antitrust liability solely under the FTC's directive.

#### 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 about 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.

#### Normal means allocates money to the FTC.

Becky Chao and Ross Schulman 20. Fellow at New America’s Open Technology Institute, former Millennial Public Policy Fellow at OTI, former honors paralegal at the Federal Trade Commission Bureau of Competition, BA in Public Policy from Duke. Senior counsel and senior policy technologist at New America’s Open Technology Institute, JD magna cum laude from American University, BS in computer science from Brandeis University. “Promoting Platform Interoperability”. New America. May 13 2020. https://www.newamerica.org/oti/reports/promoting-platform-interoperability/

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.

#### Privacy enforcement fails because the FTC’s broke.

John McGinnis and Linda Sun 21. George C. Dix Professor at NU. Associate, Wilmer Pickering Hale & Dorr LLP; JD from NU Law. “Unifying Antitrust Enforcement for the Digital Age”. 78 Wash & Lee L. Rev. 305. Winter 2021. Lexis. [Language edited].

The FTC needs more resources to adequately address the nation's growing privacy concerns. 317Currently, the FTC oversees both consumer protection--encompassing privacy--and antitrust, 318making the FTC the chief federal agency on privacy policy and enforcement 319and the nation's de facto privacy agency. 320 The agency has long-standing experience in enforcing privacy statutes 321and also has special privacy assets, such as an internet lab capable of high-quality tech forensics to track invasions of privacy. 322 The FTC, however, has failed to keep pace with the massive growth of privacy concerns--a phenomenon also driven by modern technology. 323Very few Americans feel confident in the privacy of their information in the digital age. 324According to a 2019 study, over 80 percent of Americans feel that they have little to no control over the data collected on them by companies and the government. 325To adequately address privacy concerns, the FTC needs more resources. 326 The agency has been explicit that it needs more manpower to police tech companies. 327 In requesting increased funding from Congress, FTC Director Joseph Simons said the money would allow the agency to hire additional staff and bring more privacy cases. 328 A former director of the FTC's Bureau of Consumer Protection, which houses the privacy unit, has called the FTC "woefully understaffed." 329

As of the spring of 2019, the FTC had only forty employees dedicated to privacy and data security, compared to 500 and 110 employees at comparable agencies in the U.K. and Ireland, respectively. 330 Without more lawyers, investigators, and technologists, the FTC will be forced to conduct privacy investigations less thoroughly, and in some cases, forgo them altogether. 331Currently, the FTC's resources are spread thin across multiple missions, to the detriment of its privacy efforts. Removing the agency's antitrust responsibilities would reallocate resources from the antitrust department to its privacy unit and other areas of consumer protection. 332Further, it would free up the scarce time of the commissioners to oversee this essential effort. 333

#### 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.

## extra

### add-on – multilat – 2ac

#### Splinternet collapses governance of every existential risk.

Feldstein ’20 [Steven and Peter Pomerantsev; February 10; Senior Fellow at the Carnegie Endowment for International Peace’s democracy, conflict, and governance program; Senior Fellow at the SNF Agora Institute at Johns Hopkins University where he co-directs the Arena Initiative; American Purpose, “Democracy Dies in Disinformation,” <https://www.americanpurpose.com/articles/democracy-dies-in-disinformation/>]

President Joe Biden says he wants to renew America’s democratic alliances. He has outlined a new foreign policy agenda, which aims to reinvigorate democratic values and provide stronger competition to rising authoritarian powers. His administration writes about fighting kleptocracy and climate change, conquering inequality, and standing up for human rights. There’s talk about a “Summit for Democracy” to promote the new agenda.

None of it can succeed, though, without an information environment that allows arguments to be won with evidence and allows citizens to deliberate about significant issues in a full, free, and fair conversation. Such an environment does not exist today in the United States or most other democracies.

Donald Trump’s defining technological legacy was to demonstrate the vulnerability of citizens of democracies to digital exploitation. As President, he displayed a shrewd ability to manipulate our fractured information environment to his personal advantage, promoting a mix of extreme voices that inflamed polarization and nearly propelled him to a second term.

Our authoritarian adversaries, meanwhile, are busy pursuing their own information strategies. China and Russia have defined their “cyber sovereignty” agendas, based on the idea that countries are entitled to make their own rules for governing the internet even if those rules violate universal principles like human rights. U.S. efforts to oppose them have so far been contradictory

and confused.

Trump may have ramped up rhetorical confrontation with China. In private, however, he undercut his public posture, telling Xi Jinping that the Chinese ruler should “[go ahead](https://www.wsj.com/articles/john-bolton-the-scandal-of-trumps-china-policy-11592419564)” with the building of concentration camps for Uighurs. Unsurprisingly, Trump’s messaging failed to unite democratic allies around a common agenda. When Trump did push back against the Chinese tech industry, he [adopted some of the same practices](https://www.scmp.com/comment/opinion/article/3105716/forcing-tiktok-sale-us-taking-page-out-chinas-playbook) for which he had criticized Xi, like impulsively banning China’s WeChat and TikTok apps from the U.S. market and pressing TikTok to offer itself for sale to a Trump [political supporter](https://www.vox.com/recode/2020/9/14/21437060/tiktok-trump-us-oracle-bytedance-china).

Trump tried to portray our tech competition with China as a matter of “their side” or “our side;” but since the sides were not defined by common values or even interests, it just looked like bullying, with no power to win over allies. Instead, many in the EU started to view China and America as equally bad options.

After Biden’s presidential victory, the EU [leaked a memorandum](https://www.ft.com/content/e8e5cf90-7448-459e-8b9f-6f34f03ab77a) arguing that national tech policies should be unified by “shared values.” Incoming Secretary of State Antony Blinken has said something [similar](https://www.washingtonpost.com/technology/2020/11/16/biden-huawei-trump-china/), describing “techno-democracies” that must work together to defend their values against the world’s “techno-autocracies.” But what are these values? Do we know what a democratic information environment looks like anymore?

It used to be pretty easy to define the difference between a democratic information environment and a dictatorial one. They had censorship and state-controlled media; we had freedom of speech, pluralism, and the “marketplace of ideas.”

Today, in contrast, dictators don’t just censor by constraining the amount of media content: They exploit freedom of expression to flood the environment with so much disinformation that the truth is swamped, a sort of censorship through noise. Some of the most egregious cases occur in democracies like Brazil or the Philippines. Even in Russia and China, leaders don’t just restrict communication but overload or flood information channels. Pluralism, meanwhile, displays a polarization so extreme that it destroys the possibility of a shared reality, let alone a “marketplace of ideas.”

Delineating Rights

America, of course, is in no position to lecture anyone on the subject of disinformation or tech regulation. Instead, there is a risk that democracies will fracture even further, into “splinternets,” unable to coordinate norms and standards. If so, it will become still easier for authoritarians to set their own rules. Or, if the EU continues with projects like its proposed digital regulations to govern data privacy, platform accountability, and the economic power of “gatekeeping” internet companies, the process could shift Europe away from the U.S. tech sphere. In fact, if growing numbers of countries see little cost to devising their own rules, the world could see a cyber race to the bottom.

The best current ideas in this field come from smaller frontline states, like Estonia and Taiwan, for which finding a way to design an open yet secure information environment is often existential. But without the United States, it will be hard to make real progress.

# 1ar

## platforms advantage

#### FTC expertise solves – plan isn’t a universal interoperability mandate, data security defenses could be litigated during adjudication. That’s Sharma, AND...

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

Adding it all together: Law, code, and competition

The large platforms that are subject to new interoperability requirements will need to be held accountable: they should not be allowed to pass off subpar services, or unfairly deny access to competitors by invoking the language of user protection. But policy architects should let platforms decide how to engineer their systems to meet these requirements.

Despite the flaws in the feudal privacy system, nobody is more qualified to make judgments about security threats than the platforms themselves, and platforms must be nimble to address emergent threats to their systems’ integrity. Some third-party services may prove to be bad actors, either misusing user data or neglecting to maintain secure systems, and large platforms should be able to cut off access to these legitimate threats.

Navigating this tension—between the platforms’ undeniable technical expertise and knowledge about their own systems and their anti-competitive incentives—is key to making the whole thing work. Policymakers must try to realign the incentives of big platforms to match those of their users. It’s profitable to undercut competitors, so there must be large enough penalties for anti-competitive mischief to negate those profits. There also must be sufficient transparency so that it is possible to uncover that mischief. Likewise, penalties for violating user privacy, through negligence or intent, must be severe enough to offset the money that companies stand to make by doing so. And if a company violates a user’s privacy rights, then the user should have a private right of action so they can sue the company.

#### Markets don’t solve.

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

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.

## T

#### Counterinterp – expand means to increase the scope. Their card is about density of homes in trailer parks – obvi no intent to define.

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

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

## Da

#### No AI impact---safeguards solve. Good AI inevitable

Adam **Morton 18**. Visiting Emeritus Professor of Philosophy at the University of British Columbia. 10/15/2018. “One: Escape from Earth?” Should We Colonize Other Planets?, John Wiley & Sons.

This is the best case I can make of an existential threat to humanity from intelligent machines. But now I must debunk it. Although the robot threat is often given as a reason why we should establish colonies beyond Earth, I have no doubt that the threat is exaggerated. I see three weak places, and one interestingly ambiguous topic, in the fear thus raised. First, there is the distinction between hardware and software. Computers can design other computers, because their programs were designed by other programs that have been successful at designing programs for designing programs. Or they can actually build them. An automated computer-making factory could do both, and they could be closely integrated. But these can be kept apart. Computers can be unplugged; simpler fallback software can be activated; alternative “checks and balances” software can be developed, to be put into use in times of crisis. Second, we can test software before putting it into the physically real world. The most promising means would be specific programs that probe the recesses of proposed software in order to detect just this phenomenon. (They would be vaguely analogous to the immune system in human physiology.) We can create an artificial reality in which software can operate so that its long-term devious potentialities can emerge. The software we are investigating does not have to “know” that it is not operating in the real world. These measures are also far from infallible, but they do reduce the probabilities. Recent developments in integrating human and computer proofs of mathematical theorems may well play an important role in this.

#### Openness diversifies data sets – it’s necessary for fair AI.

Natalia Norori et. al 21. Health data researcher at University of Bern, MS in Epidemiology from Bristol. Qiyang Hu, Research Scientist in computer vision and deep learning at INAIT, PhD in Computer Vision from Bern. Also Florence Marcelle Aellen, Francesca Dalia Faraci, and Athina Tzovara. “Addressing bias in big data and AI for health care: A call for open science”. Patterns. Volume 2, Issue 10. October 8 2021. Accessed thru ScienceDirect.

Data gaps

Over the past decade, governments, funders, and institutions have worked together to promote open data sharing. As a result, the world has access to public datasets to train AI algorithms, but most of them are not diverse, disaggregated, and interoperable.49 Data repositories have substantially increased the number of open datasets available to train and develop algorithms, but vulnerable populations remain underrepresented in health care data. This lack of diversity restricts the utility and generalizability of the datasets and the AI algorithms trained with them. In addition, lack of consistency and coherency, differences in formatting, and limited data disaggregation prevent open datasets from being intermixed and used to power large, complex systems.

Developing inclusive technologies relies on counting people in, but gaps in data tend to leave certain groups unnoticed. When minority groups are invisible in datasets used to deploy AI algorithms, their needs and phenotypes may become invisible. As an example, commercial, and also open genomic databases, like the Personal Genome Project, contain data that are in their vast majority of European origin.49 The lack of genetic data for large parts of the human population might hinder the development of biomarkers and treatments for conditions with a heavy genetic component.

To characterize datasets, it is important to collect comprehensive metadata. As an example, despite numerous initiatives to include sexual orientation and gender identity in electronic health records, to date this information is largely missing.50 In the vast majority of medical records it is thus impossible to identify LGBTQ+ individuals, who experience health disparities, and may have unique health care needs. Moreover, information related to the researchers or clinicians who collected certain metadata is also often missing, and its importance is ignored. Labels associated with medical data, disease rating scales, and diagnosis may be imbued with cognitive biases of the health care personnel who collected this information.51 Personality traits like tolerance to risk, or overconfidence may result in diagnostic, therapeutic, or management errors, and may impact patient outcomes.44

Data standards and interoperability

Standardization makes data interoperable and impactful. When data are not openly available and are published in inconsistent and incompatible formats, it becomes difficult to exchange, analyze, and interpret them. Inconsistency in data sharing, variability in data quality, and different levels of data usability determine whether or not researchers get access to high quality training datasets for fair AI.52

Importantly, several of the underlying datasets that power AI algorithms were not built for this purpose. As a result, the data standards (or lack of) applied to these datasets limit the potential of the algorithms that are trained with them. This is a major limitation in many of the datasets published in data science websites, such as Kaggle, where binary gender fields, incomplete gender disaggregation, and incompatible formats make it difficult to not only build inclusive AI, but also to test for biases.

Apart from formatting, data standardization can encourage patient groups to capture their characteristics in a way that facilitates readability and interoperability. For data standards to reflect those who are ultimately impacted by their adoption, broad and active participation from members of different sectors and communities is required during all steps of their design process.

To become interoperable, datasets need to track and measure inclusivity, have the possibility to exchange samples, and have clear structures that are capable to support multiple systems. Creating data standards is a complex process, but also a mandatory point of passage for training fair AI algorithms. In the fast-paced field of AI, it sometimes might be better to adopt existing standards instead of creating completely new ones.