Statement before the House Judiciary Committee
Subcommittee on Antitrust, Commercial and Administrative Law
On Online Platforms and Market Power, Part 3: The Role of Data and Privacy in Competition

Data and Privacy Inquiry: Control Points in Technology and Policy

Roslyn Layton, PhD
Visiting Scholar

October 18, 2019

Chairman Nadler, Ranking Member Collins, Subcommittee Chairman Cicilline, Ranking Member Sensenbrenner, and members of the subcommittee, thank you for the opportunity to discuss digital markets. It is an honor. I am heartened by your bipartisanship. I commend the detailed and focused preparation by committee staff in advanced of this hearing. If Congress is to make meaningful and appropriate laws, it must undertake these inquiries. Digital markets are complex field, and there is value to mapping its many dimensions and inviting different perspectives. This testimony reflects my own views and research carried out at Denmark's Center for Media and Information Technologies at Aalborg University. As a mother of three Danish-American children who are European citizens, I also have a personal and academic interest in why European policies are failing to stimulate European-made internet innovation and reducing consumer trust online.

The objectives of this digital markets inquiry are to (1) document competition problems in digital markets, (2) examine whether dominant firms are engaging in anticompetitive conduct, and (3) assess whether existing antitrust laws, competition policies, and current enforcement levels are adequate to address these issues. Additionally, the subcommittee seeks feedback on how and whether data either enable or deter market entry and how privacy may affect competition and antitrust enforcement.

Digitization challenges traditional antitrust analysis because of complexity and change.[1] Indeed the writings of Judge Louis Brandeis have been popularized of late to justify new-fangled antitrust approaches to large technology companies. However, just as Brandeis was skeptical about so-called big business, he was also concerned about big government.[2] As such, it is inconsistent to advocate dismantling enterprise while growing government.

Interestingly, Brandeis' key argument against large enterprise was that it was inefficient, but that critique does not describe today's technology firms, which are extremely efficient. These companies are highly innovative, continue to increase output, and deliver increasing value to end users. It is not in their interest to behave anticompetitively—at least in an *overt* way. However, I am concerned about their *covert* practices, their activities that do not in themselves rise to the level of antitrust violations but lead to conditions and settings that favor their continued dominance. Namely, I am concerned about how they influence public choices on internet policy and technology. Moreover, some large American tech firms have put Americans' safety, security, and privacy by bending to the will of the Chinese government in requiring data processing in China and with Chinese tools.

I will use the engineering concept of control points to describe this covert behavior. Just as a linchpin keeps a wheel from sliding off the axel, harnessing a control point is a powerful, efficient way to govern a system. As these platforms grow and gain economies of scale, the more easily they manage control points in the system, adding more capability with seemingly less effort. One need not control the system if one can just manage its control point. I will describe how the companies leverage control points in technology and public policy to gain advantages in the marketplace. Moreover, I will demonstrate how regulatory interventions, however well-intentioned, such as data protection, privacy regulation, and net neutrality, have strengthened the market positions of these companies. Many well-meaning policies are promoted on the

premise that they will "level the playing field," but we must look at the actual effects, not just the theory.

Moreover, I am skeptical to opportunistic, election season, media-seeking calls to break up "big tech". I am hard-pressed to find successes from government intervention. For example, American folklore alludes to the 19th-century railroads as justification for regulatory intervention, but the creation of the Interstate Commerce Commission itself was a product of rent seeking, reflecting the political prioritization of powerful agricultural interests over that of transport, not consumers.[3] The government intervention in Microsoft changed little; Microsoft is today the largest technology company on earth with more than $1 trillion in market capitalization. Perhaps the most successful intervention was one that never happened--IBM. New modes of computering are what bested Big Blue, not enlightened regulators.

Consider telecommunications. The Bell Telephone Company and the American government agreed on a regulated national monopoly to ensure "universal service" in 1913. Regulators were tasked with setting prices to ensure "fairness." Naturally the regulator that wanted to protect the entity on which its existence was predicated, so Bell earned excessive profits. However, consumers suffered unnaturally high prices and could only buy their phone from approved carriers. Finally, the Department of Justice broke up the collusion. However, competition was ultimately driven by new technologies in cable and mobile wireless, not governmental intervention.

The airline industry followed a similar pattern. Until deregulation in 1978, airlines in America operated under a government sanctioned oligopoly, a cartel for airmail delivery, passenger routes, and transport rates. Partial deregulation of the airline industry in the US and sunset of its outdated regulation led to a 45% decline in consumer airline ticket prices from 1978 to 2008, a doubling of passengers, a quantum leap in airline productivity, and the emergence of low-cost carriers.

It's hard to see past the dominance of the large tech-platform companies today -- but if we regulate them like monopolies, they will be around a lot longer than without the help of regulation. Today's tech giants came to prominence with better products and services that unseated their heavily regulated rivals in television, radio and print. Yet once the web firms gained critical mass, they blocked potential competitors through classic telecom rules like "network neutrality" obligations and anti-discrimination policies that were applied to the telecom operators but not to them. These rules have given the tech titans a free ride along the information highway. They force consumers to pay the full cost of their communications, rather than have it subsidized with advertising. Just as ads let Google and Facebook offer free services, it could lower the price of internet service. This innovation would give advertisers credible alternatives to the reigning platforms. That's why the tech giants and their globally coordinated advocates have fought vehemently against it, aborting its birth by lambasting it as "non-neutral". The rules were designed by the internet industry and maintained for its benefit. But such "regulatory capture" is not abnormal. Economic history is replete with eye-popping examples of sector-specific regulations that perpetuated monopolies rather than tempered their dominance.

As we can see some 18 months after the promulgation of the European Union's exalted General Data Protection Regulation (GDPR), Google, Facebook, and Amazon have gained market share while their fledgling ad tech rivals have lost ground. Only the largest players can afford the GDPR's costly requirements for lawyer fees, staff hires, software updates, and 45 other requirements. Many studies suggest that European consumers are worse off from the GDPR. The EU's morass of privacy laws, regulations, directives, and disclaimers are not lessening data breaches or the proliferation of Chinese apps, which operate in brazen defiance of European rules.

Policies such as GDPR, net neutrality and other misguided regulation have strengthened Silicon Valley dominance, and the California Consumer Privacy Act (CCPA) will likely extend it further. If we want the reign of the platforms to end, we should accelerate the rollout of new technologies and lower barriers to entry to new technologies such as 5G, artificial intelligence, blockchain, and so on.

Technology as a Control Point

A company's governance of control points, whether they are in the platform's network or not, can strengthen a platform. Control points are not the same as network effects, the increased value that a platform enjoys as more people use it. The governance of control points is an important component of understanding the complexity of online systems. I will provide examples of control points including operating systems, developer tools, digital book pricing, third-party contracts, and the DoH, the so-called domain name server (DNS) over secure hypertext transfer protocol (HTTP), unilateral efforts by Google and Mozilla to subsume a vital part of internet protocol into their proprietary networks.

Google, Facebook, Amazon, and Apple offer platforms or digital ecosystems with a foundational architectural superstructure on which modules or applications can be added to extend the services. This co-creation among the platform owner, users, and developers tussles between generative innovation and infrastructure control.[4] Some of these generative characteristics include leverage (the extent to which tools make possible a set of activities that would be impossible or prohibitively expensive otherwise), adaptability (the scope of uses tools can be put to and the ease to which they can be modified to extend this range of uses), mastery (ease to adopt tools by a broad audience), accessibility (ease of access to the tools and the information on how to use them), and transferability (degree to which the instrument can be deployed for new uses).[5]

While many radio, TV, and print outlets blame online players for displacing and disrupting their revenue, online platforms have improved the experience for consumers and advertisers. They have also expanded the media market, creating entirely new channels of distribution out of ones and zeros. More broadly, online players have invested billions of dollars to attract users and to make the online experience compelling, while many brick-and-mortar retailers have failed to make the physical shopping experience more pleasant and convenient. It feels like work to drive to a mall, find a parking space, walk a long distance to a store in surroundings

with offending music and lighting, and then interact with a disinterested employee.[6] Indeed, it is personalization based on personal information that makes the online experience compelling and convenient.

However, personalization is not unique to the online world. Many can remember the shop-keeper who recognized you, knew which products to recommend based on your relationship, and tailored unique offers to you based on your preferences. The difference today, of course, is that the knowledge of relationship is documented in code and strengthened with other sources of information. It was possible to do this in the past, but it was costly and time-consuming. Moreover, many forms of consumer tracking today did not exist in the past, notably mobile device tracking. Indeed, online brands are attempting to build a brick-and-mortar presence with their coded knowledge.[7]

Some suggest that the ability to amass data itself is a barrier to competition; however, today's innovators and entrepreneurs have multiple ways to access large databases whether free, open source projects, or via commercial databases. Indeed, there are significant costs and risks to warehouse data, and many firms find it preferable to purchase data in the market, rather than host the data themselves.

Access to data is important for machine learning. Leading financial analyst and physicist Richard Windsor explains that while media hype focuses on the killer apps of new technologies that

> . . .it's the smaller, simpler and deadly dull projects that are likely to see real success in the short to medium-term. . . boring things like saving money on electricity and basic automation where the money is going to be made. . . Deep learning, at its heart, is a system for statistically separating characteristics of data such that when these characteristics occur again, they can be recognized. . . Furthermore, the algorithm needs to be shown every combination and permutation that is possible before it can be relied on with 100% accuracy. This means that the ideal task needs to have both a finite and a stable dataset in order for deep learning to work well.[8]

A similar concern is expressed that some platform owners have disproportionate ability to mine their own data warehouses. However, this can't be true in all cases because platforms make much of their proprietary data and capabilities available through application program interfaces (APIs). The analog example is the grocery story that creates a house brand or white label brand based upon information it has about its customers and vendors. However, not all product categories are successes, and stores may focus on quality rather than price.[9]

Control Point Examples in Digital Markets

The operating system (OS) is the software that supports a computer's basic functions. Operating systems were originally designed as digital operating manuals; they did not collect or track user behavior for marketing purposes. Developers use operating systems to access baseline data about the workings of an application. This information is frequently called telemetry: data

to monitor performance remotely, especially crashes and errors. Finding and improving deficiencies help improve the system through patches, updates, and successive versions. Transforming the operating system from a mere analytics dashboard to a commercial marketing system is part and parcel of the realization of modern smartphones. While may antitrust discussion focus on the monopoly of Android-enabled devices, many forget that Android replaced the Nokia smartphone with its Symbian operating system, a platform that many thought was unbreakable. With 5G, we can begin to see creative destruction as smartphones will be supplanted by the Internet of Things.

Operating systems are the subject of considerable conflict. The Apple iOS platform ecosystem offers a rich field for research with millions of devices, over half a billion users, and millions of apps. An information systems analysis examined 4,664 technical articles published from 2007 to 2011 on the topic of contested innovation on the iOS operating system.[10] Some 30 incidents were cited as disputes between Apple and other actors over "boundary resources," the interface between the platform and developer. These incidents emerged over time, and many are ongoing today and reflect the general nature of the rivalry over sharing resources, notably Apple's rules about the language in which third-party apps must be written, how to migrate its customer base to new devices and systems, and even controversial judgments about whether some apps are politically unacceptable.

Android, by far the world's most popular operating system, has been the focus of antitrust investigations abroad related to the bundling of the operating system with Google's suite of applications, the legality of derivative versions of the operating system, and alleged exclusionary licensing of its operating system. The efficacy of these approaches in promoting innovation and alternatives remains to be seen, and there are some questions as to whether the EU properly applied competition law.[11]

The Android OS serves as the "brain" of a device containing the information of the system, all the inputs and outputs of the device, notably the log of calls and messages and the bank of photos, videos, contacts, and calendar. Android records the users' keystrokes, words, and viewed images. Android sees the information a user types before it is encrypted. Android sees the decrypted message once it's received. Android sees all browsing data, the URLs entered, search terms, pages visited and specific clicked items, logins, time spent on content, file uploads and downloads, IP address, bookmarks, app user history, and more. It has location history such as the device location, coordinated with cell tower information, Wi-Fi, and Bluetooth.

Android's capabilities extend to data collected by sensors, webcams, microphones, and any other mobile attachments. In the earlier versions, app developers were able to access, profile, and track "persistent" identifiers such as the Android ID, International Mobile Equipment Identity number,[12] hardware addresses, and SIM serial card number.[13] The advertising ID is the user's digital marketing fingerprint that is consistent across the apps and devices they use. With the "advertising ID" asset, Android can work more closely with app developers and advertisers to provide more relevant advertising to the user and monetize the experience. Android assigns

unique and global advertising identifiers, more comprehensive than cookies, to devices and allows apps to access that unique identifier for each device running the operating system.[14] These data are collected and processed from users, both to make the systems and applications work better and to provide insights to advertisers. Data from the operating system may be combined with personal data from other systems for marketing, research and development, and so on. For these reasons, the Android operating system can be provided to the end user without an out-of-pocket cost.

Facebook offers interesting jurisdictional questions because most of its users are outside the United States, and it attempts to tailor many of its offerings to local tastes. It hosts a variety of points of control that both enable users and developers to engage and share and allow Facebook to impose discipline. Facebook hosts many competing applications in platform, such as YouTube, Twitch, games, monetary transaction, and music. These apps can be experienced without leaving Facebook. While users enjoy the experience because they like to share it with their friends, it allows Facebook to capture additional personal data that can be used for ad monetization. Given the platform's capabilities, which can allow content to go viral, Facebook is constantly managing distribution, and it is critiqued on the one hand for not immediately blocking fake accounts or for not immediately stopping violent, terrorist content and on the other for not distributing social content widely enough. Facebook has made major investments in human and artificial intelligence for content and developer moderation, but it appears that the platform grows faster than its capability to manage, and the company has suffered in its earnings as a result.[15] Facebook's internal limitations and shortcomings represent opportunities for competitive alternatives. Hill Holliday's survey of Generation Z (those born since 1994) shows that so-called digital natives, who are estimated to comprise 40 percent of U.S. consumers by 2020 and of whom more than 90 percent use social media platforms, found that more than one-half had switched off social media for extended periods and one-third had canceled their social media accounts.[16] Users cited time wasting as the reason for quitting twice as often as a concern about privacy. While service providers don't like the high rates of churn on their platforms,[17] they are indicative of a competitive market in which consumers find it easy to leave and try other platforms with different features.

Amazon's relentless focus on data has reinvented the retail experience and provides an important source of competition to Google in product search. Amazon was able to incubate with a unique set of factors such as the investors who were comfortable with losses while it gained market share and profitability; the dearth of sales tax; brick-and-mortar competitors that shouldered many labor, environmental, and other regulations it did not; and regulatory decisions that deterred retailers from mergers that would have otherwise increased its competition. Amazon's control points include digital book pricing, an area in which it attempted to be price maker, but a challenge from publishers has changed how prices are negotiated.[18] As a platform for third parties, Amazon faces conflicts over contract terms, alleged cannibalization with white label products, and proliferation of banned, unsafe, and mislabeled products.[19] Similar concerns have been raised around Amazon Web Services (AWS), for example that it mines the data of retailers for insights to improve its own ecommerce.[20] However a bad rap for AWS is boon to its competitors IBM, Oracle, Virtustream, Microsoft, CenturyLink, RackSpace, and others which can

set up service level agreements to avoid such practices.

The notion of control points embraces "co-opetition,"[21] the idea that firms both cooperate and compete in the marketplace and suggests that firms and industries converge, develop, and create value in unexpected ways.[22] To describe this process David Teece's 1986 paper "Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy"[23] is essential. He observed that most innovations are not products themselves. They must be combined with complementary assets before they can be marketable products. Such partnerships lower barriers to entry and provide rewards to an innovator upfront.

Firms make partnerships or "join complementary assets" (e.g., content provider and broadband provider) to make applications known. Most applications on their own have little to no value, or will almost never be found, unless they are joined with their complementary asset. Thus, a specialized asset may be an operating system that runs on a mobile phone, such as Apple iOS or Android. A co-specialized asset may be a 4G mobile network for the Apple iPhone, its complementary asset. Many iPhone features cannot be realized unless the phone is connected to the appropriate 4G mobile network (e.g., Siri or Uber).

Marketing is a type of complementary asset. For many firms the cost on getting online is nominal: fees of hosting, storage, and servers. Where they face major barriers may be competition from other content, applications, and services, not to mention being findable on platforms such as search engines, social platforms, and app stores. The practices of search engine optimization and app store optimization are designed to help firms overcome these intermediaries.

Further, Teece's paper attempts to predict whether the innovator will succeed. To determine who wins, one needs to examine (1) appropriability—how easy is it to leverage knowledge, ease of imitation, intellectual property, etc.—and (2) complementary assets—who owns what (generic, co-specialized, or specialized). Teece also distinguishes between invention and innovation (ability to do something better than the state of the art), the latter of which adds value to users and economy. This is analogous to incremental and fundamental innovation.

Teece observes that innovating firms frequently fail to win the profits of their innovation and that the owner of the intellectual property does not necessarily get the benefit. It goes instead to customers, suppliers, or competitors—the actor which has the best fit of complementary assets. He gives the examples of EMI having developed the CAT scanner but competitors succeeding to commercialize it; RC Cola having developed diet soda but both Coca-Cola and Pepsi succeeding; Bowmar introducing the calculator but HP and Texas Instruments commercializing it; and Xerox developing the fundamental innovations that Apple managed to commercialize.

To overcome this, incumbent firms would be wise to get a position in the complementary asset market. Frequently it is not the firm that is first to market that wins, but rather that which is third, fourth, and so on. In any case, the need to work with complementary firms is reflected in the presence of joint ventures, coproduction agreements, cross-distribution arrangements, and technology licensing.

Teece also describes two stages of scientific evolution, the pre-paradigm stage and the paradigm stage. In the pre-paradigm stage, there are competing ideas, and designs are fluid. In the paradigm stage, designs become accepted, codified, and standardized. One design emerges as best (e.g., Model T, IBM 360, Douglas DC-3). Once design emerges, competition shifts to price away from design. Scale and capital then become important. Innovation can still occur but may be in niches. This model tends to characterize large consumer markets.

Few industries have the benefit of strong appropriabilities. Most of the time the appropriability is weak, so the innovator needs a business model to make its innovation known. In the pre-paradigm stage, innovators need to allow their designs to "float" to get enough of a market test to see whether they can work. In the pre-paradigm stage, the focus is on the winning design. Production is low (few users), so it does not yet make sense to deploy specialized assets. There are no scale economies, and price is not necessarily an issue. With the move to the paradigm stage, investment becomes irreversible. Once the design becomes standardized, then the importance of complementary assets takes over.

Marketing and distribution are a key complementary asset. This was demonstrated with the PC market. Many companies made computers, but few succeeded because of the scale required to sell to companies across the US (i.e., need a large sales force, get on retail shelves, etc.). So, the strategy is to sell to the big provider (e.g., IBM). In any case, Teece concludes that strategic partnerships frequently do not work for the reasons he cites.[24]

IBM's success in the PC market was related to joining the complementary assets, many of them generic. It made more sense for IBM to find them in the market than to develop them in-house. IBM's key asset relative to the generic inputs was its strong brand, which engendered credibility with customers, plus its formidable marketing and distribution network.[25]

Complementary assets are not a one-size-fits-all solution; rather it requires that each actor pursue the relevant partnership. This contrasts to the overrated policy prescription of data portability. While porting a phone number from one mobile operator to another may make sense, data from a social network do not necessarily map to an online marketplace.[26] An economic experiment with college students in the EU found that data portability was their least valued "right" of the GDPR.[27] This speaks to the lack of testing and evidence before the adoption of the GDPR and a common mistake made by policy elites to assume that users desire their preferred solutions. Instead policymakers should focus on ensuring that the marketplaces encourage innovation and experimentation.

DoH in the Mozilla and Chrome Web Browser

Another control point is the DNS, the naming system for computers, services, or other resources connected to the internet or a private network. Normally, DNS is a separate service from the platform, but platforms can also exert control on points outside their network.

DNS is characterized as a feature of the decentralized and modular architecture of the internet. Many different entities provide DNS service, and it is at the forefront to fight cyberattacks,

block malicious traffic, and limit the spread of child exploitation, terrorism, and other illegal activities. DNS is also the technology that allows parents to exercise controls to protect their children and families and a range of privacy-enhancing tools that are deployed today. DNS also enables the content delivery network industry.

One of the many privacy-enhancing technologies is encryption, techniques for secure communication in the presence of third parties. Encrypted internet traffic has hit an all-time threshold of over 72 percent of all network traffic, up from 55 percent in Q3 of 2017.[28] Google has been leading the charge for encryption, and while its operating system can see the data before and after it is encrypted, it encrypts its browser traffic so that no other parties can see it.

With a simple update to their code, Google can bypass the user's local DNS and send encrypted traffic to the central Google or Mozilla server instead, as Mozilla recently announced it plans to do soon in the US.[29] While we should encourage technological efforts to improve privacy, DoH puts even more of the internet under Google's domain and dramatically changes the internet's decentralized character. Google and Mozilla[30] offer that the move is a mere default setting to which the user can opt out and that they offer parent DNS solutions and "safe search" options. Undoubtedly, DoH makes business sense for Google and Mozilla, and some users may welcome the change. However, the furtive nature of the rollout appears to violate the spirit of the multi-stakeholder internet community. Security analysts have observed that centralizing traffic to Google's or Mozilla's DNS creates a new but needless central point of attack, breaks many parental controls, disrupts enterprise content filtering solutions, and interferes with malware detection systems. Moreover, it can exacerbate challenges for law enforcement, which has hitherto relied on DNS information. However, the lucrative new opportunities for global data monetization by large platforms is likely driving the DoH effort.

AEI's Shane Tews observes:

> Centralized encrypted DNS is a new model of internet business that goes beyond online advertising; it's a play by companies looking to exploit user behavior for their own monetary gain, cloaked as an effort to improve security and privacy. Of course, the information in these transactions can also be shared or sold with various unnamed third parties for predictive analytics and other purposes.[31]

It is not clear whether disadvantaged parties could take legal action against Google and Mozilla for an activity that turns off their traffic in an instant, but it exemplifies that vast power that can be wielded, outside of the platforms, with a mere coding tweak.

Public Policy as a Control Point

Technology can create lock-in effects but can be overcome by innovation and design. Policy and regulation, on the other hand, are more powerful control points because they can be cemented by rule of law.

Data Protection and Privacy Regulation

A policy control point is the EU's GDPR. It stipulates that any entity in the world using a European's data must comply with 45 specific regulations including hiring a chief privacy officer; purchasing a GDPR compliant software system; submitting annual audits and impact assessment to the authorities; at users' request, delivering services to users without their participation; and, at moment's notice, producing, rectifying, erasing, or transferring a user's data, among other requirements. European politicians proffered that this regime would level the playing field with Big Tech and put users in control, but 18 months after its implementation, we find that largest US tech firms have *increased* their market share, the ad tech competitors of these firms have lost market share, many small- and medium-sized (SMEs) firms have exited, and Europeans' trust online is at the lowest point since 2006. Less than half of all applicable firms comply given the high cost, some $3 million per firm. Indeed, the data protection authorities are flooded with complaints, many generated by bots, and moreover most complaints focus on billing issues with financial and retail providers, which are already covered under other laws. Europeans rarely exercise any of their 17 newly invented data protection "rights."

Since the implementation of the GDPR, Google, Facebook, and Amazon have increased their online advertising market share in the EU.[32] Three things have happened.[33] First, the high cost of GDPR compliance is a fixed cost; large, profitable firms can absorb this, but it falls harder on SMEs. Second, many advertisers and publishers have stopped using tracking tools that compete with Google and Facebook, giving a greater share of the market to the established players. Third, users are less likely to try new platforms and tools, sticking instead with the "devil they know" in the incumbent players because they perceive that the larger companies have more resources to comply with the regulation.

The GDPR has affected the downstream advertising market as well. Given the scope of Google's advertising platform and its affiliates on syndicated networks, its compliance with the GDPR has caused ripple effects in ancillary markets. Independent ad exchanges noted prices plummeting 20 to 40 percent.[34] Some advertisers reported being shut out from exchanges.[35] The GDPR's complex and arcane designations for "controllers" and "processors" can ensnare third-party chipmakers, component suppliers, and software vendors that have never interfaced with end users, as European courts have ruled that any part of the internet ecosystem can be liable for data breaches.[36] One online publisher called the GDPR the "Google Data Protection Regulation" and explained, "We have suddenly become even more dependent on Google, while other exchanges are hurting."

For those who study the empirical outcomes of regulation, the GDPR's perverse outcomes are surprising. As Nobel economist George Stigler observed more than 40 years ago, "Regulation is

acquired by industry and operated for its benefit."[37] There was an expectation that large fines would deter the platforms' business, that companies would be less aggressive in data collection, and that a space would open for small firms, but as *Politico* reported, large firms with financial and regulatory resources have "gamed" the system. Rules that were supposed to empower citizens have instead helped "Big Tech."[38]

However, disruptive innovation which would allow startups to topple the giants is probably not the goal of most European policymakers. Instead these elites likely prefer a predictable, long-lasting, and *highly regulated* oligopoly under government control conforms to their ordoliberal preferences. This contrasts with American notions of a free and fair marketplace in which startups have a shot for success without being unduly burdened by regulation. That fact that so many Europeans entrepreneurs come to the US to launch their business is a testament to this fact.

Some 40,000 internet startups in the US were founded in 2018 alone.[39] However, this a staggering number is likely to fall with the promulgation of the CCPA, what I call the GDPR-heavy because it adds 77 new regulations to enterprise, 22 more than the GDPR. The largest platforms would prefer to extend the GDPR to the US, rather than to adopt the CCPA, which has some overlapping but slightly different provisions. Indeed, Microsoft has reportedly asked US policymakers for the GDPR to be extended.[40] When large players start asking for regulation on themselves, their motivation is probably not to create competition in their own market.

The California Department of Justice and Office of the Attorney General recently issued a cost benefit analysis of the CCPA legislation and its own supplementary regulation. It notes the total initial compliance cost of $55 billion, 1.8 percent of California's gross domestic product in 2018, and another $16 billion in the coming decade.[41] About half of surveyed firms expect costs to run between $100,000 and $1 million, with vast majority of the fees going for legal services. The report also notes that 99 percent of California companies have fewer than 500 employees, meaning that costs will fall hardest on the firms with the least amount of resources and employees.[42]

Even with sophisticated modeling and economic projections, there are no scenarios in which benefits either meet or exceed costs with the CCPA. The most generous models suggest consumer benefit could amount to $1.6–$5.4 billion over time based on experiments in which consumers report willingness to pay for privacy features. Other cost benefit models suggest conservatively that the costs of the CCPA exceed benefits by a factor of four.[43]

As such, the policy will be a drag on the economy and is likely to hasten the SME exodus from the state. For a state that bills itself as a progressive leader, California is transferring massive wealth to the privacy and plaintiff bars, key advocates for the CCPA. If the goal was to help consumers, then it would be better to provide rebates to customers than fees to lawyers. The report reiterates the findings of the GDPR with the expectation of a similar impact with the CCPA noting,

> Small firms are likely to face a disproportionately higher share of compliance costs relative to larger enterprises. Conventional wisdom may suggest that stronger privacy regulations will adversely impact large technology firms that derive most of their revenue from personal data, however evidence from the EU suggests the opposite may be true. Over a year after the introduction of the GDPR, concerns regarding its impact on larger firms appear to have been overstated, while many smaller firms have struggled to meet compliance costs. Resources explain this dichotomy as large technology companies are often several steps ahead of both competitors and regulators.[44]

When startups and small players exit, existing large companies which can afford to comply will take the market share of the firms that exited. This is what happened in the EU and is what will happen in California if the CCPA is not preempted. Academic studies of other industries over time have noted that entry regulation is a barrier to entrepreneurship.[4546]

Not only can complex regulation reduce enterprise, it tricks consumers into believe the marketplace is trustworthy. Indeed "complex regulatory frameworks create the illusion of a well-controlled system," notes a recent report of Scientific Board of the European Financial Systemic Risk Board.[47] Similar unintended consequences have been noted in other industries, particularly banking and finance as the report describes,

> Excessively complex regulations contribute to increased systemic risk in several ways. First, complex regulatory frameworks create the illusion of a well-controlled system, while at the same time creating incentives for regulated entities to game the system. Second, such a framework risks missing contingencies that are not well understood, e.g. because of a lack of historical experience. An "over-fitted" regulatory system may not be well equipped to address "unknown unknowns". Third, when risks materialize, the combination of hard-to-understand interactions between different regulations and a wide array of regulatory tools can make policy responses convoluted and difficult to judge. It can also hamper the accountability of regulators and supervisors. Finally, excessive regulatory complexity can encourage the transfer of risks to institutions outside the regulatory perimeter, creating an environment where systemic risk is amplified more than it would have been if risks had remained within the perimeter.[48]

Public policy should promote firms to use data, not punish them for improving products and services for their customers. Indeed, the trouble with today's economy is not that there is too much use of data, but too little. A lack of "information intensity" is holding back the so-called other 70 percent of American economy, sectors such as transportation and health care, the latter of which consumes almost one-fifth of gross domestic product.[49] Outside of certain applications, the traditional healthcare industry is woefully inefficient; digital industries, on the other hand, are eight times more productive and innovative. If the US does not innovate these other sectors, other nations will beat us to it. China is already on track with an "Internet Plus" policy which supports the digitization of industries, including healthcare and government.[50]

While policies such as the GDPR and CCPA claim to promote competition, they both have the effect of increasing barriers for new market entrants and reducing competition. When they were founded, Google, Amazon, Facebook, Apple, and Microsoft enjoyed permissionless data collection and processing innovation; the next wave of innovators will not. So, we can only expect to drag out the dominance of these large firms which now enjoy government-promoted protection from competition. A detailed discussion of the effects of the GDPR and CCPA is submitted to the subcommittee in a separate report, as it exceeds time allotted this hearing.

Internet Regulation

Public policy is a salient control point in the marketplace, and its value is so well established that is has been enshrined by Tullock's paradox.[51] It notes that the cost of rent-seeking is small relative to the gains.[52] While the size of the public affairs budgets of the big tech companies can make for an interesting story or two in the press, a few million dollars is relatively little compared to their total operations, which number in the trillions of dollars. It makes good economic sense for the companies to spend a few million on public affairs to win favorable public policy, for the costs of developing fundamental innovation and associated products and services is in the billions. For more than a decade, control point subterfuge by the tech companies fooled policymakers into thinking that America's 5,441 internet service providers were a threat internet openness. The entire US broadband industry, some $300 billion, is still smaller than the market capitalization of any one of the internet giants. And still, many policymakers have supported a distorted notion that the internet giants should be shielded from competition.

My doctoral research investigated net neutrality policy across 53 countries during the period of 2010–16 to test the hypothesis that countries that adopt hard, bright line net neutrality rules should experience an increase in locally developed mobile app development innovation in their national economy.[53] Following the net neutrality tenets, I expected to see those countries adopting rules would experience greater competition to established edge providers. However, I discovered the opposite. In fact, net neutrality in practice works to cement the market position of existing giants. In no country that has adopted hard net neutrality rules have we seen any platforms emerge to challenge Google, Facebook, or Amazon. In fact, the only places that has produced meaningful competitors to these firms are Russia and China, and these countries have no net neutrality rules at all. If we followed the net neutrality predictions, we should have seen global platforms emerge from Brazil and India, which have had hard net neutrality rules for years. Tomasso Valletti has also described the ambiguous effects of this policy.[54]

Google, Amazon, Facebook, Microsoft, and to a lesser degree, Apple, have lobbied hard in the US and other countries on this issue. They have succeeded to enshrine the norm that disproportionately large senders of traffic pay little to nothing for the cost of networks while the end user pays the full network cost regardless of whether she visits those sites. Moreover, the policy restricts competition by prohibiting startups and end users the freedom to partner to tailor ser-

vices to their individual wants, needs, and budgets. If it was not for the Noerr-Pennington doctrine, which allows the industrial sector to work collectively for favorable price controls, these platforms would likely be guilty of collusion and restraint of trade.

Policy Considerations

Stop Promoting Regulation That Strengthens the Largest Players

If we are concerned about competition and market entry, we must stop making high-cost policies that give Big Tech an unfair advantage. This testimony documents how many well-intentioned regulations delivered the opposite of their intended effect. The high cost of compliance has turned into a market barrier that only the richest companies can afford. As a result, nascent competitors have either stagnated or exited the market while the large companies gained market share. I urge Congress not to adopt the GDPR, or its US imitator, the CCPA, whose financial impacts are likely to be even more detrimental to the US than the GDPR is to Europe.

If the California law is promulgated, it will likely be challenged in court on free speech grounds and will ultimately be struck down as unconstitutional. Moreover, the CCPA threatens to torpedo more than two-dozen hard-fought privacy laws with existing regimes and regulators overseeing the health and insurance sectors, to name just two industries. To keep the US from devolving into 50 conflicting layers of privacy regulation and destroying interstate internet commerce, Congress should preempt the CCPA with evidence-based policy instrument that complement, not supplant, existing law.

Rational Privacy Protections

Evidence-based policy is a rational, linear process to make decisions based upon an evaluation of problems and possible solutions, the collection of information about the possible solutions, and the measurement and comparison of expected outcomes. Had California used an evidence-based approach, it would have conducted randomized, controlled trials to test the efficacy of the 185 provisions rather than slop together a laundry list of feel good rules, as it did over a few weeks.[55] The policy process should be informed by competing approaches with associated assessments *before* legislation is made, not after. Ideally the bill would undergo Congressional scoring and/or review by the Office of Management and Budget for additional rigor.

I appreciate the efforts of this committee, notably Ranking Member Collins,[56] to explore rational, rule-of-law-based methods to protect consumers' privacy and encourage innovation without burdening small- and medium-sized enterprise. Such an approach preserves Constitutional rights and freedoms including interstate commerce; honors the single national market created by our founders; and protects the legal system from rent-seeking and abuse by the plaintiff bar and litigation financiers who wish to profit off the largesse of the tech industry. Most consumers never the rents of class action lawsuits, as winnings go overwhelmingly to the attorneys bringing the cases.[57]

Congressman Collins' proposal[58] dovetails with the "Privacy Bill of Rights" presented by the

2012 Obama White House, a sound privacy framework built on the principles of individual control, transparency, respect for context, security, accuracy, and accountability and strengthened enforcement at the Federal Trade Commission (FTC). [59] President Obama's proposal supported using multi-stakeholder processes to develop enforceable codes of conduct through Section 5 of the FTC Act. Moreover, the Obama administration was adamant about the need for preemption of state laws that would contradict the national standard. Plan architect Cameron F. Kerry describes how it would have functioned,

> The bill of rights articulated seven basic principles that should be legally enforceable by the Federal Trade Commission: individual control, transparency, respect for the context in which the data was obtained, access and accuracy, focused collection, security, and accountability. These broad principles are rooted in longstanding and globally-accepted "fair information practices principles." To reflect today's world of billions of devices interconnected through networks everywhere, though, they are intended to move away from static privacy notices and consent forms to a more dynamic framework, less focused on collection and process and more on how people are protected in the ways their data is handled. Not a checklist, but a toolbox. This principles-based approach was meant to be interpreted and fleshed out through codes of conduct and case-by-case FTC enforcement—iterative evolution, much the way both common law and information technology developed.[60]

Sadly, Silicon Valley thwarted this visionary plan.[61] It is likely that had the US adopted this plan in 2012, it would have beat the EU to the privacy punch and avoided much of the current state of fallout.

University of Washington Law professor Jane Winn offers a helpful overview of US information law, noting how the US focused on risk-based laws which allow innovation except where risk justifies precaution versus the EU where the bureaucracy administers unilateral control rights.[1] She explains that the US approach is an attempt to strike a balance between the public demand for protection from harm with the public demand growth and innovation, and making legislation when there is a clear misuse of information to harm individuals. Citing the low rate of compliance of EU firms with information laws (both the 1995 EU Data Protection Directive and the GDPR), Winn explains that European governments and businesses have an "attitude of calculated indifference toward the challenge of achieving real compliance" and reluctance to compete on digitization. She observes, "American businesses are more likely than their European counterparts to try to use technology innovation as a source of competitive advantage."

Winn describes important historical points where consumer choice and business innovation have allowed the United States to emerge as the global leader in making digital transformation accessible to individuals and the punctuating legislation. For example in prior centuries, one of the first things European immigrants did upon arriving to the US was to borrow money for new

[1] Winn, Jane, The Governance Turn in Information Privacy Law (July 11, 2019). Available at SSRN: https://ssrn.com/abstract=3418286

clothes so that they could blend in with Americans.[2] "Consumerism and the power to construct a new identity with consumer credit remain inextricably woven into the fabric of American democracy," she writes. When Congress enacted the world's first fair information practices law to protect American consumers' power to borrow money, the Fair Credit Reporting Act of 1970, "it was acting in response to the high level of concern among American consumers that the migration of paper credit bureau records to computers might needlessly restrict their access to credit." If there is an "fundamental right" enshrined in American legislation, it is the "right of American consumers to borrow freely to finance their present consumption…in most European countries, there is often a deep ambivalence or even hostility toward American-style consumerism and the culture of easy access to consumer credit that makes it possible," notes Winn.

A related issue in the 1970s was a deep distrust of the US government from the Vietnam War and Watergate which threatened to deter signups to the new Medicare and Medicaid programs. The Secretary of Health, Education and Welfare commissioned a report to determine what the federal government needed to do to restore trust, resulting in the groundbreaking 1973 HEW Report on Computers, Records and the Rights of Citizens and the subsequent Privacy Act of 1974 which contained the first mention of "fair information privacy practices" or FIPPS ever articulated anywhere in the world. FIPPs was "a way to restore the necessary balance between the interests of individuals in how their data is processed on the one hand, and the interests of organizations and the public generally in how that data is processed on the other." What has allowed the Privacy Act to endure is not the notion of privacy as a fundamental right of individual control (an idea it rejects), but rather the *mutual interest* of the individual and the government to maintain the accuracy and reliability of the personal information with the use of FIPPS as a guide. Congress has since made many information privacy laws for specific areas, still in effect today, depending on the harm at risk with the issue at hand. [3]

Winn advises a new framework of information governance that simultaneously addresses privacy and disclosure in a flexible, dynamic way. Congress can borrow elements of other U.S. laws that have been very successful in other contexts, such as the way the way regulators work with voluntary, consensus standards organizations to create concrete, certifiable standards for the specific business practice in question. Unlike industry self-regulation, "accredited" standards are certified by the American National Standards Institute and organizations adopting these official standards must observing the due process requirements contained in a document known as "ANSI Essential Requirements." ANSI standards are already employed today successfully

[2] Lendol Calder, Financing the American Dream: A Cultural History of Consumer Credit (1999).

[3] This includes Family Educational Rights and Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Video Privacy Protection Act of 1988, the Telephone Consumer Protection Act of 1991, the Driver's Privacy Protection Act of 1994, the Health Insurance Portability and Accountability Act of 1996, the Children's Online Privacy Protection Act of 1998, and the Gramm-Leach-Bliley Act of 1999.Other examples of risk-based information privacy laws are the Privacy Act, ERISA; the National Labor Relations Act; the Internal Revenue Act; the Bank Secrecy Act; HIPAA; the Family and Medical Leave Act; the Genetic Information Nondiscrimination Act; the 21st Century Cures Act; the Occupational Safety and Health Act; the Telemarketing and Consumer Fraud and Abuse Prevention Act; CAN-SPAM Act; Electronic Communications Privacy Act (including the Wiretap Act, Stored Communications Act and Pen Register Act; the Cybersecurity Information Sharing Act; and the Whistleblower Protection Act.

across many industries. A key advantage compared to the EU's blanket rights approach is that standards are explicit, technical, and measurable and therefore can ensure stricter compliance.

To enable the transition for the millions of firms to which the integrated, national information framework would apply, Congress could authorize federal regulators to confer "safe harbor" status to organizations adopting the rigorous standards along with limited preemption for inconsistent state laws. Notably such rules allow the FTC to impose stricter rules when warranted on certain firms and industries, rather than to saddle every startup with obligations designed for a trillion-dollar platform. Most important, Winn describes why the traditional US approach to privacy has been the best avenue to deliver democracy and actual privacy on the ground, not just on the books.

> Cloaking European-style data protection law in the language of fundamental rights short-circuits the democratic process of balancing the costs and benefits of different regulatory strategies. . . Having insulated themselves from democratic accountability with a fundamental rights narrative, EU institutions are now reaping a whirlwind of populist and nationalist movements across Europe that are openly hostile to European institutions. . . For those who have never faced the challenge of creating and sustaining a culture of compliance, EU-style data protection law appears to be a much simpler, clearer solution to the problem of information governance than a messy, ambiguous risk-based approach. It is only when the challenges of achieving actual compliance is taken into account that the democratic character of the American risk-based model becomes clear.

Congress is right to focus on competition in the tech sector, but it won't achieve this with from third rate platforms mandate by government fiat. Instead Congress should hasten the next technological revolution which will supplant the current incumbents. This can be done through policy that supports investments and incentives for next-generation technologies and removes the market barriers to entrepreneurship, innovation, and enterprise. Here the focus should be on fast-tracking 5G, the internet of things, artificial intelligence, blockchain, and security technologies.

In summary rational privacy legislation could consist of (1) framework that protects Americans' Constitutional rights and freedoms for speech and commerce; (2) strengthened authority and budget for the FTC to develop risk-based privacy standards for the online economy (this would also include budget for more economists and technologists at the agency); (3) safe harbors that allow companies to migrate their operations to those standards, (4) investments and incentives for the development of privacy-enhancing technologies, and (5) consumer education and competency training.[62]

I am heartened by the bipartisanship in Congress today with the opportunity to make a meaningful framework that builds on proven American success and scientific evidence. I thank the committee for this opportunity to testify, its willingness to engage a range of participants, and its openness to new ideas and frameworks. I look forward to your questions.

Notes

[1] Mark A. Jamison, *Applying Antitrust in Digital Markets*, September 9, 2019, https://ssrn.com/abstract=3427450.
[2] Brandeis, L. D., & Lewis, C. M. (1934). *The Curse of Bigness: Miscellaneous Papers of Louis D. Brandeis*. Viking Press.
[3] Roslyn Layton, "Avoiding the Regulatory Bait and Switch of Common Carriage," AEIdeas, April 25, 2019, http://www.aei.org/publication/avoiding-the-regulatory-bait-and-switch-of-common-carriage/. See also Jenny Bourne, *In Essentials, Unity: An Economic History of the Grange Movement* (Ohio University Press, 2017).
[4] Ben Eaton et al., "Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System," *MIS Quarterly: Management Information Systems* 39, no. 1 (2015): 217–43.
[5] Ben Eaton, Silvia M. Elaluf-Calderwood, and Carsten Sørensen, "The Role of Control Points in Determining Business Models for Future Mobile Generative Systems," IEEE, 2010.
[6] Omar Abbosh, Paul Nunes, and Larry Downes, *Pivot to the Future: Discovering Value and Creating Growth in a Disrupted World* (PublicAffairs, April 23, 2019).
[7] Flavio Palaci, Ramy Sedra, and Anand Rao, "Digital-Native Retailers Are Giving Physical Stores a Radical Makeover," Strategy+Business, January 18, 2019, https://www.strategy-business.com/article/Digital-Native-Retailers-Are-Giving-Physical-Stores-a-Radical-Makeover?gko=7f0a1.
[8] Richard Windsor. "Artificial Intelligence – Dull delivers." Radio Free Mobile. September 5, 2019. https://radiofreemobile.com/2019/09/05/artificial-intelligence-dull-delivers/
[9] Hoch, S. J., & Banerji, S. (1993). When do private labels succeed?. *MIT Sloan Management Review*, *34*(4), 57.
[10] Supra Eaton 2015
[11] Bergqvist, Christian and Rubin, Jonathan, Google and the Trans-Atlantic Antitrust Abyss (March 18, 2019). University of Copenhagen Faculty of Law Research Paper No. 2019-73. Available at SSRN: https://ssrn.com/abstract=3354766
[12] The International Mobile Equipment Identity is a number, usually unique, to identify 3GPP and iDEN mobile phones and some satellite phones.
[13] John E. Dunn, "Thousands of Android Apps Bypass Advertising ID to Track Users," Sophos, February 19, 2019, https://nakedsecurity.sophos.com/2019/02/19/thousands-of-android-apps-bypass-advertising-id-to-track-users/.
[14] Android Software Development Kit, "Android Software Development Kit License Agreement," Android, http://developer.android.com/sdk/terms.html; Tune Help, "Google's Advertising Identifier," February 21, 2014, https://help.tune.com/marketing-console/googles-advertising-identifier/; and Apple SDK agreement.
[15] Richard Windsor, "Facebook—the Long Hard Road," Radio Free Mobile, June 3, 2019, http://radiofreemobile.com/2019/06/03/facebook-the-long-hard-road/.
[16] Hill Holliday, Meet Gen Z: The Social Generation, http://thinking.hhcc.com/?utm_campaign=Thought%20Leadership%20%E2%80%94%20Gen%20Z&utm_source=Press%20Release (last visited June 25, 2018).
[17] Connie Hwong, Why Churn Rate Matters: Which Social Media Platforms Are Losing Users?, Verto Analytics, May 4, 2017, https://www.vertoanalytics.com/chart-week-social-media-networks-churn/.
[18] Amazon, "Apple eBooks Antitrust Settlement," https://www.amazon.com/gp/feature.html?ie=UTF8&docId=1002402851.
[19] Alexandra Berzon, Shane Shifflett, and Justin Scheck, "Amazon Has Ceded Control of Its Site. The Result: Thousands of Banned, Unsafe or Mislabeled Products," *Wall Street Journal*, August 23, 2019, https://www.wsj.com/articles/amazon-has-ceded-control-of-its-site-the-result-thousands-of-banned-unsafe-or-mislabeled-products-11566564990.
[20] See
https://www.wsj.com/articles/wal-mart-to-vendors-get-off-amazons-cloud-1498037402
https://www.cnbc.com/2017/06/21/wal-mart-is-reportedly-telling-its-tech-vendors-to-leave-amazons-cloud.html
https://www.cnbc.com/2017/08/29/target-is-moving-away-from-aws-after-amazon-bought-whole-foods.html
https://www.ciodive.com/news/dramatic-or-justified-retailers-fears-push-cloud-customers-from-aws-to-mi/543273/
[21] Brandenburger, A. M., & Nalebuff, B. J. (2011). *Co-opetition*. Crown Business.
[22] Arthur H. Copeland, "Book Review: Theory of Games and Economic Behavior," *Bulletin of the American Mathematical Society* 51, no. 7 (July 1, 1945): 498–505.
[23] David Teece, "Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy," *Research Policy* 15 (June 1986), http://www4.lu.se/upload/CIRCLE/INN005/Teece_Reflections.pdf.

[24] Roslyn Layton and Silvia Monica Elaluf-Calderwood, "Zero Rating: Do Hard Rules Protect or Harm Consumers and Competition? Evidence from Chile, Netherlands and Slovenia" (Rochester, NY: Social Science Research Network, August 15, 2015), http://papers.ssrn.com/abstract=2587542.
[25] Roslyn Layton and Silvia Monica Elaluf-Calderwood, "Free Basics Research Paper: Zero Rating, Free Data, and Use Cases in Mhealth, Local Content and Service Development, and ICT4D Policymaking" (Rochester, NY: Social Science Research Network, September 27, 2016), https://papers.ssrn.com/abstract=2757384.
[26] Inge Graef, Sih Yuliana Wahyuningtyas, and Peggy Valcke, "Assessing Data Access Issues in Online Platforms," *Telecommunications Policy* 39, no. 5 (June 2015): 375–87.
[27] Maciej Sabolewski and Palinski Michal, "How Much Consumers Value Online Privacy? Welfare Assessment of New Data Protection Regulation (GDPR)" (International Telecommunications Society Conference, Passau, July 31, 2017).
[28] John Maddison, "More Encrypted Traffic Than Ever," Fortinet Blog, December 10, 2018, https://www.fortinet.com/blog/industry-trends/more-encrypted-traffic-than-ever.html.
[29] Selena Deckelmann, "What's Next in Making Encrypted DNS-over-HTTPS the Default," Mozilla, September 6, 2019, https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/; and Zak Doffman, "Firefox Plans Controversial New Encryption Setting for Millions, and Update Starts This Month," *Forbes*, September 8, 2019, https://www.forbes.com/sites/zakdoffman/2019/09/08/firefox-announces-major-new-encryption-default-to-protect-millions-of-users/.
[30] Over 90 percent of Mozilla's revenue comes from Google, as a result of the Mozilla Firefox browser setting Google as the default search engine. It is unclear what the terms of the agreement with Cloudflare are to make them the default DoH resolver for Firefox. Cloudflare has recently filed an initial public offering. See Stephen Shankland, "Google-Firefox Search Deal Gives Mozilla More Money to Push Privacy," CNET, November 27, 2018, https://www.cnet.com/news/google-firefox-search-deal-gives-mozilla-more-money-to-push-privacy/; and Jordan Novet, "Web Security Company Cloudflare Files to Go Public," CNBC, August 15, 2019, https://www.cnbc.com/2019/08/15/cloudflare-s-1-ipo-filing.html.
[31] Shane Tews, "Should Big Tech Be the Sole Operator of the Internet's Domain Name Infrastructure?," AEIdeas, June 25, 2019, http://www.aei.org/publication/should-big-tech-be-the-sole-operator-of-the-internets-domain-name-infrastructure/.
[32] Mark Scott, Laurens Cerulus, and Laura Kayali, "Six Months in, Europe's Privacy Revolution Favors Google, Facebook," *Politico*, November 27, 2018, https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/. Other articles that discuss this include Sam Schechner and Nick Kostov, "Google and Facebook Likely to Benefit from Europe's Privacy Crackdown," *Wall Street Journal*, April 23, 2018, https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324; Alex Webb, "Google's Mortal Enemy Does It a $95 Billion Favor," Bloomberg, July 20, 2018, https://www.bloomberg.com/opinion/articles/2018-07-20/google-s-mortal-enemy-does-it-a-95-billion-favor; and Alex Webb, "Google and Facebook Turn on the Fake Riviera Charm," Bloomberg, June 25, 2018, https://www.bloomberg.com/opinion/articles/2018-06-25/google-and-facebook-turn-on-the-fake-riviera-charm.
[33] James Campbell, Avi Goldfarb, and Catherine Tucker, "Privacy Regulation and Market Structure," *Journal of Economics & Management Strategy* 24, no. 1 (2015): 47–73.
[34] Jessica Davies, "'The Google Data Protection Regulation': GDPR Is Strafing Ad Sellers," Digiday (June 4, 2018), https://digiday.com/media/google-data-protection-regulation-gdpr-strafing-ad-sellers/.
[35] Catherine Armitage, "Life After GDPR: What Next for the Advertising Industry?," World Federation of Advertisers, July 10, 2018, https://www.wfanet.org/news-centre/life-after-gdpr-what-next-for-the-advertising-industry/.
[36] European Union, Judgment of the Court (Grand Chamber), June 5, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62016CJ0210&qid=1531145885864&from=EN.
[37] George Stigler, "The Theory of Economic Regulation," *Bell Journal of Economics* 2, no. 1 (1971): 3–21.
[38] Mark Scott, Laurens Cerulus, and Steven Overly, "How Silicon Valley Gamed Europe's Privacy Rules," *Politico*, May 22, 2019, https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/.
[39] TIA Cyberstates 2019
[40] Andrea O'Sullivan, "Now Microsoft Supports an American GDPR. Which Tech Giant Wouldn't?," *Reason*, May 28, 2019, https://reason.com/2019/05/28/now-microsoft-supports-an-american-gdpr-which-tech-giant-wouldnt/.

[41] Berkeley Economic Advising and Research, "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," State of California Department of Justice Office of the Attorney General, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

[42] Ibid p. 31

[43] Roslyn Layton. "The costs of California's online privacy rules far exceed the benefits." AEIdeas. March 22, 2019. https://www.aei.org/technology-and-innovation/the-costs-of-californias-online-privacy-rules-far-exceed-the-benefits/

[44] Supra Berkeley p. 31

[45] Klapper, L., Laeven, L., & Rajan, R. (2006). Entry regulation as a barrier to entrepreneurship. *Journal of financial economics*, *82*(3), 591-629

[46] Kotsios, P. (2010, March). Regulatory Barriers to Entry in Industrial Sectors. In *International Conference on International Business*.

[47] "Regulatory complexity and the quest for robust regulation." European Financial Systemic Risk Board. Reports of the Advisory Scientific Committee. No 8. June 2019.

[48] Supra p. 2

[49] Bret Swanson. "Securing the Digital Frontier: Policies to Encourage Digital Privacy, Data Security, and Open-Ended Innovation." AEI. May 2019. https://www.aei.org/research-products/report/securing-the-digital-frontier-policies-to-encourage-digital-privacy-data-security-and-open-ended-innovation/

[50] http://english.gov.cn/premier/news/2015/03/13/content_281475070887811.htm

[51] Tullock, G. (1967). The welfare costs of tariffs, monopolies, and theft. *Economic Inquiry*, *5*(3), 224-232.

[52] Krueger, A. O. (1974). The political economy of the rent-seeking society. *The American economic review*, *64*(3), 291-303

[53] Roslyn Layton, *Which Open Internet Framework Is Best for Mobile App Innovation? An Empirical Inquiry of Net Neutrality Rules Around the World*, Aalborg Universitet, 2017, https://doi.org/10.5278/vbn.phd.engsci.00181. A summary is available at Roslyn Layton, "Does Net Neutrality Spur Internet Innovation?," American Enterprise Institute, August 23, 2017, https://www.aei.org/research-products/report/does-net-neutrality-spur-internet-innovation/.

[54] Greenstein, S., Peitz, M. & Valletti, T. (2016). *Net Neutrality: a fast lane to understanding the trade-offs.* NBER Working Paper 21950.

[55] See Eric Goldman, "An Introduction to the California Consumer Privacy Act (CCPA) (July 9, 2018)," Santa Clara University, https://ssrn.com/abstract=3211013 or http://dx.doi.org/10.2139/ssrn.3211013.

[56] Doug Collins, "Collins Releases Principles to Protect Online Data Property and Privacy," House of Representatives Judiciary Committee, July 10, 2019, https://republicans-judiciary.house.gov/press-release/collins-releases-principles-to-protect-online-data-property-and-privacy/.

[57] Martin Redish, Wholesale Justice: Constitutional Democracy and the Problem of the Class Action Lawsuit. Stanford Books, 2009. https://www.amazon.com/Wholesale-Justice-Constitutional-Democracy-Stanford/dp/0804752753

[58] Doug Collins, "Collins Releases Principles to Protect Online Data Property and Privacy," House of Representatives Judiciary Committee, July 10, 2019, https://republicans-judiciary.house.gov/press-release/collins-releases-principles-to-protect-online-data-property-and-privacy/.

[59] Office of the Press Secretary, "We Can't Wait: Obama Administration Unveils Blueprint for a 'Privacy Bill of Rights' to Protect Consumers Online," White House, February 23, 2012, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

[60] Cameron F. Kerry. "Why protecting privacy is a losing game today—and how to change the game." Brookings. Thursday, July 12, 2018 https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

[61] Natasha Singer, "Why a Push for Online Privacy Is Bogged Down in Washington," *New York Times*, February 28, 2016, https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

[62] Layton, Roslyn, How the GDPR Compares to Best Practices for Privacy, Accountability and Trust (March 31, 2017). Available at SSRN: https://ssrn.com/abstract=2944358