July 16, 2019

The Honorable David N. Cicilline
Chairman
Subcommittee on Antitrust,
Commercial and Administrative Law
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

The Honorable F. James Sensenbrenner
Ranking Member
Subcommittee on Antitrust,
Commercial and Administrative Law
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Cicilline and Ranking Member Sensenbrenner:

The Electronic Frontier Foundation (EFF) is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation. With over 30,000 dues-paying members and well over 1 million followers on social networks, we focus on promoting policies that benefit both creators and users of technology. We support the Subcommittee's efforts to analyze the competitive landscape when it comes to the Internet marketplace and wish to submit the following EFF publications to aid those efforts.

Historically, the power of the Internet arose from its edges: innovation, growth, and freedom came from its users and their contributions, rather than from some centrally controlled core of overseers. But today, for an increasing number of users, there is a powerful center to the net—and a potentially uncompetitive and unrepresentative center at that.

As a whole, the Internet is still vast and complex, enabling billions of users to communicate regardless of their physical location. Billions of websites, apps, and nearly costless communications channels remain open to all. Yet too many widely relied-upon functions are now controlled by a few giant companies. Worse, unlike previous technology cycles, the dominance of these companies has proven to be sticky. It's still easy and cheap to put up a website, build an app, start a business, or organize a group of people online—***but a few large corporations dominate key resources needed to do those things.*** That, in turn, gives those companies extraordinary power over speech, privacy, and innovation. Congress's investigation into why this has happened is critical and we support your efforts.

Sincerely,

Electronic Frontier Foundation

Interoperability: Fix the Internet, Not the Tech Companies

By Cory Doctorow

Everyone in the tech world claims to love interoperability—the technical ability to plug one product or service into another product or service—but interoperability covers a lot of territory, and depending on what's meant by interoperability, it can do a lot, a little, or nothing at all to protect users, innovation and fairness.

Let's start with a taxonomy of interoperability:

Indifferent Interoperability

This is the most common form of interoperability. Company A makes a product and Company B makes a thing that works with that product, but doesn't talk to Company A about it. Company A doesn't know or care to know about Company B's add-on.

Think of a car's cigarette lighter: these started in the 1920s as aftermarket accessories that car owners could have installed at a garage; over time they became popular enough that they came standard in every car. Eventually, third-party companies began to manufacture DC power adapters that plugged into the lighter receptacle, drawing power from the car engine's alternator. This became widespread enough that it was eventually standardized as ANSI/SAE J563.

Standardization paved the way for a variety of innovative new products that could be made by third-party manufacturers who did not have to coordinate with (or seek permission from) automotive companies before bringing them to market. These are now ubiquitous, and you can find fishbowls full of USB chargers that fit your car-lighter receptacle at most gas stations for $0.50-$1.00. Some cars now come with standard USB ports (though for complicated reasons, these tend not to be very good chargers), but your auto manufacturer doesn't care if you buy one of those $0.50 chargers and use it with your phone. It's your car, it's your car-lighter, it's your business.

Cooperative Interoperability

Sometimes, companies are eager to have others create add-ons for their products and services. One of the easiest ways to do this is to adopt a standard: a car manufacturer that installs an ANSI/SAE J563-compliant car-lighter receptacle in its cars enables its customers to use any compatible accessory with their cars; any phone manufacturer that installs a 3.5mm headphone jack allows anyone who buys that phone to plug in anything that has a matching plug, even exotic devices like Stripe's card-readers, which convert your credit-card number to a set of tones that are played into a vendor's phone's headphone jack, to be recognized and re-encoded as numbers by Stripe's app.

Digital standards also allow for a high degree of interoperability: a phone vendor or car-maker who installs a Bluetooth chip in your device lets you connect any Bluetooth accessory with it—provided that they support that device, or at least that they make no steps to prevent that device from being connected.

This is where things get tricky: manufacturers and service providers who adopt digital standards can use computer programs to discriminate against accessories, even those that comply with the standard. This can be extremely beneficial to customers: you might get a Bluetooth "firewall" that warns you when you're connecting to a Bluetooth device that's known to have security defects, or that appears on a blacklist of malicious devices that siphon away your data and send it to identity thieves.

But as with all technological questions, the relevant question isn't merely "What does this technology do?" It's "Who does this technology do it *to* and who does it do it *for*?"

Because the same tool that lets a manufacturer help you discriminate against Bluetooth accessories that harm your well-being allows the manufacturer to discriminate against devices that harm *its* well-being (say, a rival's lower-cost headphones or keyboard) even if these accessories enhance *your* well-being.

In the digital era, cooperative interoperability is always subject to corporate boundaries. Even if a manufacturer is bound by law to adhere to a certain standard—say, to provide a certain electronic interface, or to allow access via a software interface like an API—those interfaces are still subject to limits that can be embodied in software.

A digitally enabled car-lighter receptacle could be made to support only a limited range of applications—charging via USB but not USB-C or Lightning, or only charging phones but not tablets—and software could be written to enforce those limits. Even a very permissive "smart lighter-receptacle" that accepted every known device as of today could be designed to reject any devices invented later on, unless the manufacturer chose to permit their use. A manufacturer of such a device could truthfully claim to support "every device you can currently plug into your car lighter," but still maintain a pocket veto over future devices as a hedge against new developments that it decides are bad for the manufacturer and its interests.

What's more, connected devices and services can adjust the degree of interoperability their digital interfaces permit from moment to moment, without notice or appeal, meaning that the browser plugin or social media tool you rely on might just stop working.

Which brings us to...

Adversarial Interoperability

Sometimes an add-on comes along that connects to a product whose manufacturer is outright hostile to it: third-party ink for your inkjet printer, or an unauthorized app for your iPhone, or a

homebrew game for your console, or a DVR that lets you record anything available through your cable package, and that lets you store your recordings indefinitely.

Many products actually have countermeasures to resist this kind of interoperability: checks to ensure that you're not buying car parts from third parties, or fixing your own tractor.

When a manufacturer builds a new product that plugs into an existing one despite the latter's manufacturer's hostility, that's called "adversarial interoperability" and it has been around for about as long as the tech industry itself, from the mainframe days to the PC revolution to the operating system wars to the browser wars.

But as technology markets have grown more concentrated and less competitive, what was once business-as-usual has become almost unthinkable, not to mention legally dangerous, thanks to abuses of cybersecurity law, copyright law, and patent law.

Taking adversarial interoperability off the table breaks the tech cycle in which a new company enters the market, rudely shoulders aside its rivals, grows to dominance, and is dethroned in turn by a new upstart. Instead, today's tech giants show every sign of establishing a permanent, dominant position over the internet.

"Punishing" Big Tech by Granting It Perpetual Dominance

As states grapple with the worst aspects of the Internet—harassment, identity theft, authoritarian and racist organizing, disinformation—there is a real temptation to "solve" these problems by making Big Tech companies legally responsible for their users' conduct. This is a cure that's worse than the disease: the big platforms can't subject every user's every post to human review, so they use filters, with catastrophic results. At the same time, these filters are so expensive to operate that they make it impossible for would-be competitors to enter the market. YouTube has its $100 million Content ID copyright filter now, but if it had been forced to find an extra $100,000,000 to get started in 2005, it would have died a-borning.

But assigning these expensive, state-like duties to tech companies also has the perverse effect of making it much harder to spark competition through careful regulation or break-ups. Once we decide that providing a forum for online activity is something that only giant companies with enough money to pay for filters can do, we also commit to keeping the big companies big enough to perform those duties.

Interoperability to the Rescue?

It's possible to create regulation that enhances competition. For example, we could introduce laws that force companies to follow interoperability standards and oversee the companies to make sure that they're not sneakily limiting their rivals behind the scenes. This is already a feature of good telecommunications laws, and there's lots to like about it.

But a mandate to let users take their data from one company to another—or to send messages from one service to another—should be the opener, not the end-game. Any kind of interoperability mandate has the risk of becoming the ceiling on innovation, not the floor.

For example, as countries around the world broke up their national phone company monopolies, they made rules forcing them to allow new companies to use their lines, connect to their users and share their facilities, and this enabled competition in things like long distance service.

But these interoperability rules were not the last word: the telcos weren't just barred from discriminating against competitors who wanted to use their long-haul lines; thanks to earlier precedent, they were also not able to control who could make devices that plugged into those lines. This allowed companies to make modems that could connect to phone lines. As the Internet crept (and then raced) into Americans' households, the carriers had ample incentive to control how their customers made use of the net, especially as messaging and voice-over-IP eroded the massive profits from long-distance and SMS tariffs. But they couldn't, and that helplessness to steer the market let new companies and their customers create a networked revolution.

The communications revolution owes at least as much to the ability of third parties to do things that the carriers hated—but couldn't prevent—as it does to the rules that forced them to interconnect with their rivals.

Fix the Internet, Not the Tech Companies

The problems of Big Tech are undeniable: using the dominant services can be terrible, and now that they've broken the cycle of dominance and dethroning, the Big Tech companies have fortified their summits such that others dare not besiege them.

Today, much of the emphasis is on making Big Tech better by charging the companies to filter and monitor their users.

The biggest Internet companies need more legal limits on their use and handling of personal data. That’s why we support smart, thorough new Internet privacy laws. But laws that require filtering and monitoring user content make the Internet worse: more hostile to new market entrants (who can't afford the costs of compliance) and worse for Internet users' technological self-determination.

If we're worried that shadowy influence brokers are using Facebook to launch sneaky persuasion campaigns, we can either force Facebook to make it harder for *anyone* to access your data without Facebook's explicit approval (this assumes that you trust Facebook to be the guardian of your best interests)—or we can bar Facebook from using technical and legal countermeasures to shut out new companies, co-ops, and projects that offer to let you talk to your Facebook friends without using Facebook's tools, so you can configure your access to minimize Facebook's surveillance and maximize your own freedom.

The second way is the better way. Instead of enshrining Google, Facebook, Amazon, Apple, and Microsoft as the Internet's permanent overlords and then striving to make them as benign as possible, we can fix the Internet by making Big Tech less central to its future.

It's possible that people will connect tools to their Big Tech accounts that do ill-advised things they come to regret. That's kind of the point, really. After all, people can plug weird things into their car's lighter receptacles, but the world is a better place when *you* get to decide how to use that useful, versatile ANSI/SAE J56-compliant plug—not GM or Toyota.

Fines Aren't Enough: Here's How the FTC Can Make Facebook Better

By Bennett Cyphers

The Federal Trade Commission is likely to announce that Facebook's many violations of users' privacy in recent years also violated its consent decree with the commission. In its financial filings, Facebook has indicated that it expects to be fined between $3 and $5 billion by the FTC. But punitive fines alone, no matter the size, are unlikely to change the overlapping privacy and competition harms at the center of Facebook's business model. Whether or not it levies fines, the FTC should use its power to make Facebook better in meaningful ways. A new settlement with the company could compel it to change its behavior. We have some suggestions.

A $3 billion fine would be, by far, the largest privacy-related fine in the FTC's history. The biggest to date was $22.5 million, levied against Google in 2012. But even after setting aside $3 billion to cover a potential fine, Facebook still managed to rake in $3.3 billion in profit during the first quarter of 2019. It's rumored that Facebook will agree to create a "privacy committee" as part of this settlement. But the company needs to change its actions, not just its org chart. That's why the settlement the FTC is negotiating now also needs to include limits on Facebook's behavior.

Stop Third-Party Tracking

Facebook uses "Like" buttons, invisible Pixel conversion trackers, and ad code in mobile apps to track its users nearly any time they use the Internet—even when they're off Facebook products. This program allows Facebook to build nauseatingly detailed profiles of users'—and non-users'—personal activity. Facebook's unique ability to match third-party website activity to real-world identities also gives it a competitive advantage in both the social media and third-party ad markets. The FTC should order Facebook to stop linking data it collects outside of Facebook with user profiles inside the social network.

Don't Merge WhatsApp, Instagram, and Facebook Data

Facebook has announced plans to build a unified chat platform so that users can send messages between WhatsApp, Messenger, and Instagram accounts seamlessly. Letting users of different services talk to each other is reasonable, and Facebook's commitment to end-to-end encryption for the unified service is great (if it's for real). But in order to link the services together, Facebook will likely need to merge account data from its disparate properties. This may help Facebook enrich its user profiles for ad targeting and make it harder for users to fully extricate their data from the Facebook empire should they decide to leave. Furthermore, there's a risk that people with one set of expectations for a service like Instagram, which allows pseudonyms and does not require a phone number, will be blindsided when Facebook links their accounts to real identities. This could expose sensitive information about vulnerable people to friends, family, ex-

partners, or law enforcement. In short, there are dozens of ways the great messenger union could go wrong.

Facebook promises that messaging "interoperability" will be opt-in. But corporations are fickle, and Facebook and other tech giants have repeatedly walked back privacy commitments they've made in the past. The FTC should make sure Facebook stays true to its word by ordering it not to merge user data from its different properties without express opt-in consent. Furthermore, if users do decide to opt-in to merging their Instagram or WhatsApp accounts with Facebook data, the FTC should make sure they reserve the right to opt back out.

Stop Data Broker-Powered Ad Targeting

Last March, Facebook shut down its "Partner Categories" program, in which it purchased data from data brokers like Acxiom and Oracle in order to boost its own ad-targeting system. But over a year later, advertisers are still using data broker-provided information to target users on Facebook, and both Facebook and data brokers are still raking in profit. That's because Facebook allows data brokers to upload "custom audience data files"—lists of contact information, drawn from the brokers' vast tranches of personal data—where they can charge advertisers to access those lists. As a result, though the interface has changed, data broker-powered targeting on Facebook is alive and well.

Data brokers are some of the shadiest actors in the digital marketplace. They make money by buying and selling detailed information about billions of people. And most of the people they profile don't know they exist. The FTC should order Facebook to stop allowing data brokers to upload and share custom audiences with advertisers, and to explicitly disallow advertisers from using data broker-provided information on Facebook. This will make Facebook a safer, less creepy place for users, and it will put a serious dent in the dirty business of buying and selling private information.

A Good Start, But Not the End

We can't fix all of the problems with Facebook in one fell swoop. Facebook's content moderation policies need serious work. The platform should be more interoperable and more open. We need to remove barriers to competition so that more privacy-respecting social networks can emerge. And users around the world deserve to have baseline privacy protections enshrined in law. But the FTC has a rare opportunity to tell one of the most powerful companies in the world how to make its business more privacy-protective and less exploitative for everyone. These changes would be a serious step in the right direction.

Protecting the Life Cycle of Competition

By Ernesto Falcon

The power of the Internet historically arose from its edges: innovation, growth, and freedom came from users and their contributions, rather than from some centrally controlled core of overseers. But today, for an increasing number of users, there is a powerful center to the net. The expected new entrants that will displace the giants only to be displaced by successor entrants may not come. The lack of competition and choice impacts nearly every facet of Internet users' privacy and speech rights as a small handful of giants control our access to the network and run the platforms we use there. It is time to take a hard look at whether our laws can cope with the power of dominant players and protect the ability of new entrants to emerge and displace the giants.

Antitrust

Antitrust enforcement has become strangled in an outmoded economic doctrine that fails to recognize the realities of today's Internet. Increasingly, consumers "pay" for services not in dollars, but with their personal data. In this new reality, it makes no sense to evaluate consumer welfare solely on the basis of price. Federal antitrust regulators should consider the very real costs to consumers, such as privacy practices and corporate platform censorship, and explore other levers within antitrust law such as the essential facilities doctrine. Antitrust enforcers must increase scrutiny of mergers and acquisitions by massive vertically integrated Internet companies to ensure future competition is not being snuffed out.

Competition Policy

Broadband access is quickly devolving into a national monopoly as cable companies deploy gigabit networks without facing competition. The United States lags behind the EU and advanced Asian markets on deployment of fiber to the home infrastructure, with no clear plan to reach universal competitive high-speed access. In the platform and application markets, promotion of data portability and interoperability will allow for "follow-on innovators" that can interact with and analyze existing Internet platforms as well as build on them in ways that benefit users. Decentralized, federated services gave us telephony, email, and the World Wide Web. A focus on interoperability and data portability could bring the same benefits to today's Internet users.

Consumer Privacy

Much of today's consumer frustration stems from a series of data privacy scandals that have involved big Silicon Valley companies and major Internet service providers. However, regulation that treats the giants as the same as startups and smaller companies seeking to displace them will only cement the dominant companies. EFF strongly discourages a one-size-fits-all approach to privacy rules that do not take into account the differences in ability to comply. One way to distinguish between startups and established entities is the creation of an information fiduciary rule that does not apply to new entrants but rather is triggered at a certain size and scale.

Copyright

Innovative startups are dependent on copyright's safe harbors for intermediary liability, and careful stewardship of the fair use doctrine by the judicial branch. Without clarity on liability, it would be impossible to create applications and services and manage the risk of ruinous damages. This issue arises not only for startups seeking to host user-generated content or interact with media, but for any platform that interoperates with existing technologies and formats. Copyright law currently allows copyright holders who sue for infringement to seek "statutory damages" as high as $150,000 per work. Statutory damages drive much of the distortion in copyright liability, and is in desperate need of reform so that the damage claims leveraged by litigious rights holders reflect reality and present manageable risks.

Computer Fraud and Abuse Act (CFAA)

The CFAA is a serious criminal law meant to target malicious computer break-ins. But some corporate litigants have abused the law's notoriously vague language against would-be competitors. Under the threat of civil enforcement and criminal prosecution, cease and desist letters citing the CFAA are a proven tool for scaring new entrants away. For example, industry giants currently relying on the Ninth Circuit's *Facebook v Power Ventures* decision are attempting to use the CFAA to block access to *publicly available* information on the open Internet through cease and desist letters. This fundamentally changes the open access norms that have governed the Internet since its inception and has protected their status as market leaders. They have also relied on the CFAA to block products that would have allowed consumers to manage their social media networks in one place, view information from multiple classified ads websites in one useful interface, and rely on a single messaging app to connect with all of their various messaging tools.

Intermediary Liability

Section 230 of the Communications Decency Act protects Internet platforms of all sizes from liability based on the speech of their users. Major incumbents support eroding this protection by creating new, complex obligations. Doing so would cement their dominance by reducing competition from new entrants. Congress must not further erode the safe harbor that today's platforms relied on to become the current Internet giants. Efforts to place greater liability on Internet intermediaries for the speech of their users, even in the most narrow of instances, drive up the costs of deploying an open platform. Companies must find the technology and the people power to moderate their users and the content they post, a challenge given the rapid pace at which Internet products grow if they are successful. In fact, the most recent erosion of open platform immunity, in an effort to combat sex trafficking (FOSTA/SESTA), has done nothing to alleviate the problem. Sex workers have been forced to return to the streets and into the hands of sex traffickers, while existing platforms have contracted and the cost of market entry has increased for others.