Cory Doctorow
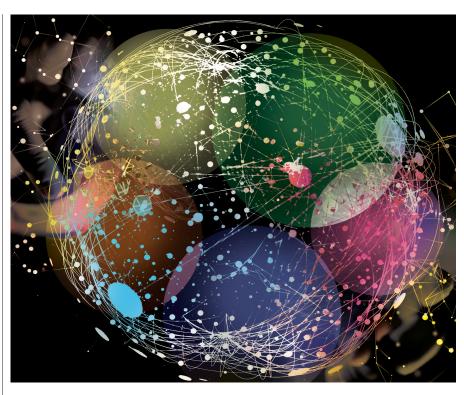
Viewpoint
Competitive Compatibility: Let's Fix the Internet, Not the Tech Giants

Seeking to make Big Tech less central to the Internet.

TECH'S MARKET CONCENTRATION— summed up brilliantly by Tom Eastman, a New Zealand software developer, as the transformation of the Internet into "a group of five websites, each consisting of screenshots of text from the other four"—has aroused concern from regulators around the world.

In China tech giants have been explicitly co-opted an arm of the state. In Europe regulators hope to discipline the conduct of U.S.-based "Big Tech" firms by passing strict rules about privacy, copyright, and terrorist content and then slapping the companies with titanic fines when they fail to abide by them. At the same time, European leaders talk about cultivating "national champions"—monopolistically dominant firms with firm national allegiance to their local governments.

U.S. lawmakers are no more coherent: on the one hand, Congress recently held the most aggressive antitrust hearings since the era of Ronald Reagan, threatening to weaken the power of the giants by any means necessary. On the other hand, lawmakers on both sides of the aisle want to deputize Big Tech as part of law enforcement, charged with duties as varied as preventing human trafficking, policing copyright infringement, imposing neutrality on public discourse, blocking disinformation, and ending harassment and hate speech. If any of these

duties can be performed (and some of them are sheer wishful thinking), they can only be performed by the very largest of companies, monopolists who extract monopoly rents and use them to fund these auxiliary duties.

Tech has experienced waves of concentration before and resolved them with minimal state action. Instead, tech's giants were often felled by interoperability, which allows new market entrants to seize the "network effect" advantages of incumbents to turn them to their own use. Without interoperability, AT&T ruled the nation. With interoperability, the ubiquity of the Bell System merely meant that anyone who could make an answering machine, radio bridge, or modem that could plug into an RJ-11 jack could sell into every house and business in America.

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 does not talk to Company A about it. Company A does not know or care to know about Company B's add-on.

You can find fishbowls full of USB chargers that fit your car-lighter receptacle at most gas stations for $0.50–$1.00. Your auto manufacturer does not care if you buy one of those $0.50 chargers and use it with your phone. It is your car, it is your car-lighter, it is 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.

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 they take 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 are connecting to a Bluetooth device that is 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 is not merely "What does this technology do?" It is "Who does this technology do it *to* and who does it do it *for*?"

The same tool that lets a manufac-

In the digital era, cooperative interoperability is always subject to corporate boundaries.

---

turer 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.

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 the browser plugin[a] or social media tool[b] you rely on might just stop working.

Which brings us to …

Competitive Compatibility

Sometimes an add-on comes along that connects to a product whose manufacturer is hostile to it: third-party inkjet ink, unauthorized iPhone apps, DVRs that record anything available through your cable package, and stores your recordings indefinitely.

Many products now have countermeasures to resist this kind of interoperability: checks to ensure you are not buying car parts from third parties,[c] or fixing your own tractor.[d]

When a manufacturer builds a new product that plugs into an existing

---

a   See https://bit.ly/3lVVPai
b   See https://bit.ly/3AB99EQ
c   See https://bit.ly/3lRnWax
d   See https://bit.ly/3scBGNZ

---

one despite the latter's hostility, that is called "competitive compatibility"[e] and it has been around for about as long as the tech industry itself, from the mainframe days[f] to the PC revolution[g] to the operating systems wars[h] to the browser wars.[i]

All three forms of interoperability share some characteristics: in each case, technologists devise a means by which two or more products or services can extend one another's functionality, read one another's files, or otherwise provide benefit to the users of one or both services.

The difference between these forms of interoperability is in the type of technical work necessary to accomplish them.

Firms that create APIs or other interfaces to explicitly invite third-party add-ons contemplate both their users' and employers' priorities and try to strike a balance between them, crafting a means whereby their inventions can be improved or adapted by others without foregoing unacceptable future revenues from making such improvements on their own.

Firms that participate in standards-setting make a similar calculus but arrive at a different equilibrium. A multistakeholder format means that if you try to standardize, say, the costs of your products (in the hopes of getting others to shoulder them), while maintaining as proprietary the sources of your profits, you will have to convince other participants (including your commercial rivals) that this is a fair arrangement. Standards Development Organizations describe these compromises as a major feature of standardization itself: rivals check one another's most greedy impulses and arrive at a fair middle ground that does not unduly advantage any one firm (of course, in highly concentrated markets, large firms can collude to create standards that advantage them at the expense of potentially disruptive new market entrants).

These "cooperative interoperability" efforts can give rise to follow-on, "indifferent interoperability" mo-

---

e   See https://bit.ly/3CEE1X7
f   See https://bit.ly/2XekFrm
g   See https://bit.ly/3xM6beN
h   See https://bit.ly/3fYllaK
i   See https://bit.ly/3yHKsWZ

ments. These occur when new products and services leverage deliberately interoperable technologies to do things that are orthogonal the considerations that went into the original. Think of the USB charger that plugs into a car's lighter receptacle: the firms that standardized the receptacle in the first place worked carefully to ensure none of their cars would be at a competitive disadvantage when it came to attracting drivers who smoked; they gave careful consideration to production, maintenance, and safety; but they did not even consider a distant future in which a universal power-cable would emerge to charge lithium-ion cells in commodity consumer electronics.

As tobacco smoking declined and device-charging grew, automakers gave more consideration to this new use case, and even encouraged it, turning indifferent interoperability into cooperative compatibility after the fact.

Unlike cooperative interoperators or indifferent interoperators, technologists engaged in competitive compatibility have an adversarial relationship with those who came before them. To defeat the anti-tampering chip in a single-use print-cartridge, or field a scraper that exports user-data from a giant's walled garden, or make a third-party office suite that seamlessly reads and writes an incumbent's spreadsheets, word processor documents and presentations, a technologist must defeat obfuscation, encryption, intrusion detection, and other countermeasures meant to thwart them.

The indifferent interoperator faces challenges that the cooperative interoperator does not. The cooperative interoperate can put in a request for an API extension, or argue in a standards committee for the inclusion of a feature they need. The indifferent operator has no leverage over the product's vendor(s), and has to work within the constraints of the product as it exists in the field.

Technologists who engage in competitive compatibility, however, are actively working at cross-purposes to those who came before them. They are playing a game of cat-and-mouse, relying on exploiting defects, or camouflaging their tools as normal user activities, and they must contend with the possibility that the result of their efforts will be revisions to the original product or service explicitly designed to break their add-ons (indifferent operators sometimes see their work undone by these updates, but only as an incidental effect and not out of any animus to them).

Competitive compatibility can also collapse into cooperative compatibility. Sometimes dominant companies surrender and agree to cooperate: today's office file formats are standardized under ISO, the proprietary HTML extensions of the browser wars have been discarded or integrated into W3C standards, and so on.

There is a reason that compatibility tends to win out over the long run—it is the default state of the world—the sock company does not get to specify your shoes and the dairy does not get to dictate which cereal you pour milk over.

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

Taking competitive compatibility off the table breaks the tech cycle: 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 is worse than the disease: the big platforms cannot subject every user's every post to human review, so they use filters, with catastrophic results.[n] At the same

j   See https://bit.ly/3scslWt
k   See https://bit.ly/3yDaMBr
l   See https://bit.ly/2XntxLw
m See https://bit.ly/3iEvECP
n   See https://bit.ly/2VPgO3c

The biggest Internet companies need more legal limits on their use and handling of personal data.

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[o] 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 open their back-ends[p] and oversee the companies to ensure they are not sneakily limiting their rivals behind the scenes. This is already a feature of good telecommunications laws,[q] and there is a lot 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.

Fix the Internet,
Not the Tech Companies

The problems of Big Tech are undeni-able: using the dominant services can be terrible, and now that they have broken the cycle of dominance and de-throning, the Big Tech companies have fortified their summits such that others dare not besiege them.[r]

The biggest Internet companies need more legal limits on their use and handling of personal data. That's why we need a national privacy law, with a "private right of action" so that users can bring suit if they are victimized by surveillant companies. But laws that require filtering and monitoring user content make the Internet worse: more hostile to new market entrants (who cannot afford the costs of compliance) and worse for Internet users' techno-logical self-determination.

If we are worried that shadowy influence brokers are using Face-book to launch sneaky persuasion campaigns,[s] we can either force Face-book to make it more difficult for *anyone* to access your data without Facebook's explicit approval (this as-sumes that you trust Facebook to be the guardian of your best interests)—or we can bar Facebook from using technical and legal countermeasures[t] 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. That would mean reform-ing the Computer Fraud and Abuse Act to clarify that it cannot be used to make Terms of Service violations into civil or criminal offenses; reforming the Digital Millennium Copyright Act to clarify that defeating a technical protection measure is not an offense if doing so does not result in a copy-right infringement; comprehensively narrowing software patents to allow for interoperable reimplementations; amending copyright to dispel any doubt as to whether reimplementing an API is a copyright infringement; and limiting the anticompetitive use of other statutes including those re-lating to trade secrecy, nondisclosure, and noncompete.

The second way is the better way.

Instead of enshrining Google, Face-book, Amazon, Apple, and Microsoft as the Internet's permanent overlords and then striving to make them as be-nign as possible, we can fix the Inter-net by making Big Tech less central to its future.

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

Corporations Make
Terrible Governments

AT&T was very nearly broken up in 1956. The monopolistic conduct that had enraged rural Americans and would-be telecoms rivals reached such an undeniable nadir that the DoJ finally moved to break up Ma Bell. Only one thing stood in the way: the Pentagon. AT&T had been deputized to perform so many state-like duties during its decades of monopolistic operations that it had acquired pow-erful stakeholders in the U.S. govern-ment—it had its own army! The Pen-tagon told the DoJ that it could not successfully occupy Korea an intact AT&T: it needed its Death Star to be a fully operational battle-station.

AT&T got a stay of execution, and instead was slapped with restrictions on its conduct that it skirted, violat-ed, and flouted for the next three de-cades, until, finally, it was broken up in 1982. That 26-year reprieve was the direct result of "fixing" AT&T by trying to co-opt it to serve the state, rather than using the power of the state to weaken it.

Government derive their power from the consent of the governed. Their legitimacy comes from their ac-countability. Companies have share-holders, not citizens. Businesses are not governments, and they have no businesses governing us. **ⓒ**

o See https://econ.st/3yIGT2J
p See https://bit.ly/3xD1DHD
q See https://bit.ly/3CIUOYN

r See https://bit.ly/2VJmRHe
s See https://bit.ly/2Xj9C05
t See https://bit.ly/3scYUn9

u See https://bit.ly/3fZ2FYD

Cory Doctorow (cory@eff.org) is Visiting Professor of Computer Science at the Open University, U.K.