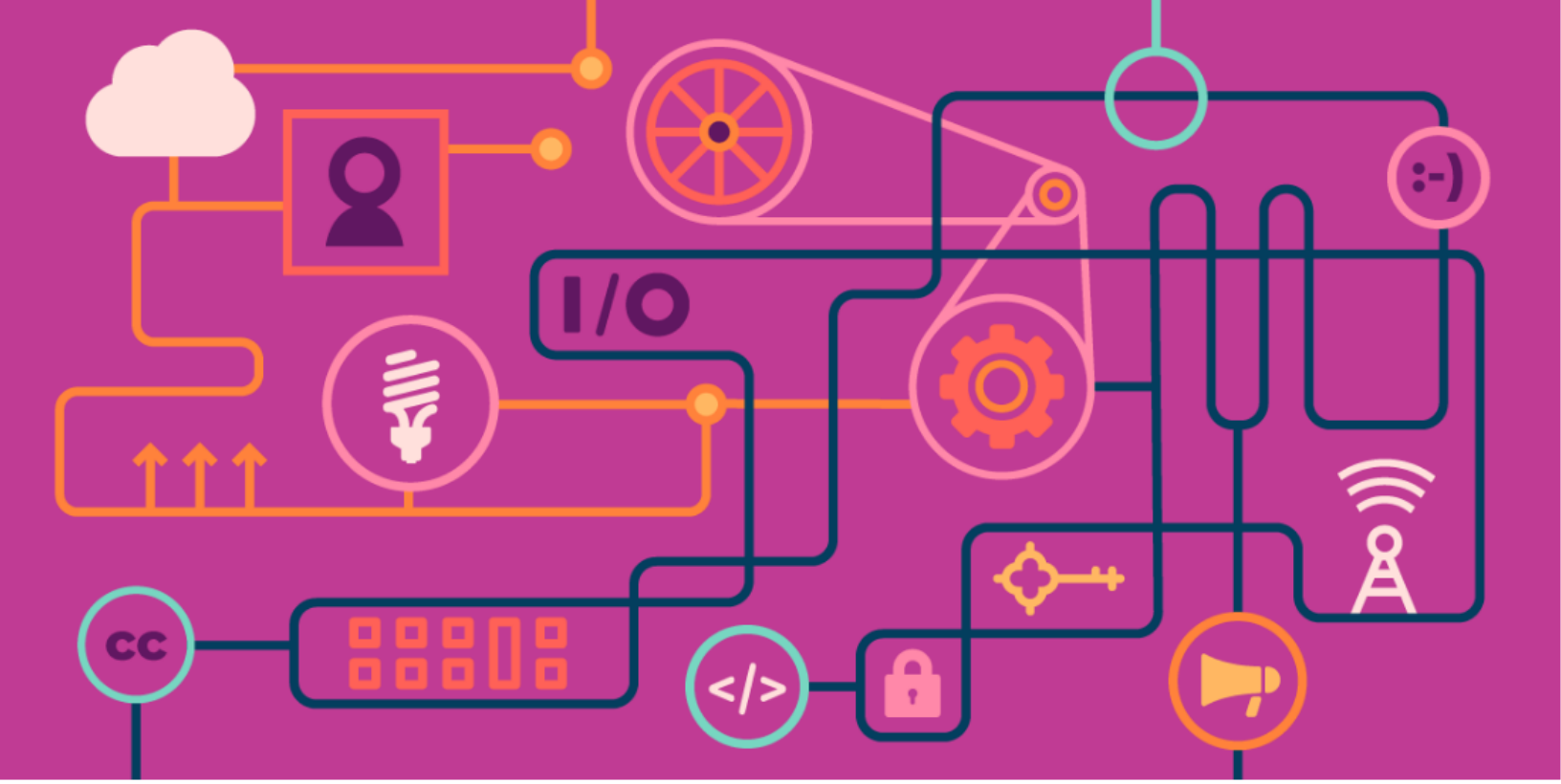

Privacy Without Monopoly

DATA PROTECTION AND INTEROPERABILITY

ELECTRONIC FRONTIER FOUNDATION

Authors: Bennett Cyphers, Cory Doctorow

A publication of the Electronic Frontier Foundation, 2021.

View this report online: https://www.eff.org/wp/interoperability-and-privacy

Privacy Without Monopoly:

Data Protection and Interoperability

Bennett Cyphers
Staff Technologist
and
Cory Doctorow
Special Advisor

February 12, 2021

Executive Summary

The problems of corporate concentration and privacy on the Internet are inextricably linked. A new regime of interoperability can revitalize competition in the space, encourage innovation, and give users more agency over their data; it may also create new risks to user privacy and data security. This paper considers those risks and argues that they are outweighed by the benefits. New interoperability, done correctly, will not just foster competition, it can be a net benefit for user privacy rights.

In **section 2** we provide background. First, we outline how the competition crisis in tech intersects with EFF issues and explain how interoperability can help alleviate it. In "**The Status Quo**," we describe how monopoly power has woven the surveillance business model into the fabric of the Internet, undermining the institutions that are supposed to protect users. Finally we introduce the "**privacy paradox**"—the apparent tension between new interoperability and user privacy—that frames this paper.

In **section 3**, we present EFF's proposals for interoperability policy.

The first is "**competitive compatibility**" or **ComCom**: encouraging tinkerers and startups to interoperate with incumbent services without their permission. A ComCom policy regime would dismantle the legal tools that corporations use to shut down interactions with their services that they don't approve of. We propose better interpretations of, and reforms to, the Computer Fraud and Abuse Act (**CFAA**), Section 1201 of the Digital Millennium Copyright Act (**DMCA**), and contract law pertaining to Terms of Service (**ToS**) and End User License Agreements (**EULAs**).

The second proposal would require some companies to provide a baseline of interoperable access to their services. **Data portability** gives users the right to access and transfer their data from the companies that hold it. **Back-end interoperability** would require very large companies—those that dominate a particular market segment—to maintain interfaces that allow their users to interact fluidly with users on other services. Finally, **delegability** would require those large companies to build interfaces that allow third-party software to interact with their services on a user's behalf.

In **section 4**, we consider the new privacy risks that these policies may create and discuss how to mitigate them.

Enabling competitive compatibility will help loosen dominant platforms' control over how their services are used. This may leave the largest companies, to whom users entrust huge amounts of sensitive data, with fewer ways to shut down third-party actors that threaten user privacy. But big tech companies have never been good stewards of sensitive user data, and the laws we propose reforming have never been the right tools to protect it. Making it easier for new entrants to create privacy-preserving

alternatives will pressure incumbents to do better, and allow users to migrate away when they don't.

New interoperability rules will create new data flows, and remove some of the platforms' discretion to decide how data is shared. But mandates can come with strings attached, in the form of legal obligations for informed consent and data minimization. As a result, data that flows across these new interfaces may be more legally protected than any data that the platforms have chosen to share in the past.

In this paper, we imagine a world where interoperability and privacy go hand in hand, and abusive monopolists are not deputized to act as a private arm of the state. We can, and should, have both competition and privacy—and users should be able to enjoy the many other benefits of interoperability as well.

1. Introduction

Internet market concentration is among the most important tech policy issues of our time. Over the past few years, a chorus of voices have begun calling for governments to intervene and rein in the tech giants' power. However, there is less consensus on how exactly that should be done without causing new problems.

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

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

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

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

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

This whitepaper outlines some EFF proposals to promote competition and innovation through interoperability. It addresses the privacy risks of these proposals and discusses how we can mitigate them and shows why, despite some new risks,

interoperability-positive policy does not have to come at the cost of user privacy. Done right, interoperability can actually protect privacy by making it easier for users to control who has their data and how it is used.

The paper is organized as follows:

Section 2 gives background about competition, interoperability, and the tension between access and privacy.

Section 3 presents EFF's recommendations for policies that will promote and establish interoperability.

Section 4 discusses privacy risks associated with these policies and proposes ways to mitigate those risks.

Section 5 concludes.

This whitepaper is not a comprehensive argument for interoperability per se. While we will give background on the competition crisis and why interoperability will help address it, we assume the reader agrees that more interoperability on the Internet is desirable, but has reservations about its effects on data privacy and security. Furthermore, this paper discusses the need for new privacy laws, but does not attempt to tackle the way privacy law should be written (see EFF's previous work for more on that). This paper is specifically focused on mitigating the privacy and security issues associated with new interoperability policy.

Although we discuss new legislation, news laws are not the only way to enact these policies. Some may fit best into a legislative agenda, while others could be given force as part of a package of litigation remedies. Better interpretations of existing law can also go a long way. Companies may even choose to voluntarily enter binding agreements to carry out these policies, possibly in order to stave off less desirable regulatory outcomes.

This paper's goal is to examine how things might change if we get the interoperability policy we want, so it's important to note what we do not want. We are not advocating for unmoderated app stores; in fact, many app distribution systems (like the Chrome web store) can and should be moderated to protect user privacy. Instead, we are against anticompetitive use of moderation power, and against a moderated app store having a monopoly on software distribution. We do not want to remove computer crime laws altogether, and companies should be able to engineer their products the way they want. But the law should not help corporations control anything and everything that goes on within their products.

2. Background

2.1. Interoperability and Competition

EFF has long argued for the right of new market entrants—commercial and nonprofit, individual and institutional—to connect their products and services to existing ones, especially dominant ones. EFF has fought for the right to scrape information and the right to modify devices, the right to block trackers and reimplement APIs, the right to repair and the rights of reverse engineers. These are the building blocks of interoperability, which has a long history of breaking market strangleholds enjoyed by dominant companies.

The market concentration crisis in tech has brought the need for interoperability into sharp focus. A number of factors have contributed to rapid, decisive centralization over the past two decades, with a handful of companies amassing unprecedented power across borders and industries. Those same factors make it highly unlikely that the tech sector will "fix itself" any time soon.

For one, network effects give the biggest player in a market a powerful advantage over smaller, newer, and even superior competitors. Social media, in particular, has become a difficult market to break into as Facebook has made itself central to more aspects of its users' lives. No one wants to join a new social media site if their friends aren't on it—and all their friends are already on Facebook (or the Facebook-acquired properties Instagram or Whatsapp). Even in markets outside of traditional "social" media, the identity graphs controlled by a handful of giants make it easy for them to muscle out competitors in everything from online advertising to document collaboration.

Of course, new companies do gain traction from time to time, usually by creating a new competitive sub-market: a chat app that delivers a better mobile experience like WhatsApp, or a dedicated visual image sharing tool, like Instagram. But for the better part of two decades, that hasn't presented a real problem for incumbents. A lax and short-sighted merger review regime in the U.S. has allowed big companies to buy up competitors at an alarming rate.

Better merger review will help, and unwinding problematic mergers from the past two decades will help more. But not all conglomerates are built through mergers, and structural separation is complicated and not guaranteed to fix the unique problems of concentration in tech.

Interoperability is a key policy for a pro-competitive Internet. Interoperability undermines network effects that keep users locked into a conglomerate's ecosystem. It removes barriers for new entrants by letting small players piggyback on the infrastructure developed by big ones. On the early Internet, the protocols everyone used to communicate (like TCP/IP and HTTP), were open and interoperable. If we can push the tech giants in that direction—towards being true platforms for others to work on top of, with, and around—then starting and growing a new co-operative or company will

get easier. Further, interoperability reduces the benefits of conglomeration, by making it harder for a big company to leverage one service to the benefit of its other holdings.

As a goal, interoperability is great: it's easy to imagine a world with lower switching costs for users, less protection for incumbents, and more innovation across the board. Interoperability is, in essence, data flow—successful policy will mean more personal data traveling more freely between servers around the world.

Getting there is more difficult. Intervening in a fast-moving set of industries like today's tech sector is never easy, and the interventions we propose need resources and finesse to execute correctly.

2.2. The Status Quo

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

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

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

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

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

2.3. The Privacy Paradox

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

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

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

3. Policy Tools to Promote Interoperability

Interoperability is everywhere. The kinds of interoperability we intend to promote—new stable interfaces to large platforms via mandates, and new competitive compatibility through better law—should both look familiar.

Many companies already invite interoperability for a variety of purposes, from allowing integration with other services to fostering secondary application marketplaces. Large platforms especially tend to offer powerful application programming interfaces (APIs) that give third-party developers access to features of their products. The interfaces created under new mandates will likely look and function like supercharged versions of the interfaces companies already choose to expose.

Likewise, competitive compatibility has long been practiced by ambitious young companies and curious independent developers alike. Gopher, the precursor to the modern Web browser, was a grand exercise in scrounging for information across the early Net. Financial aggregators like Mint started out by scraping data from bank websites on their users' behalf. And in modern browsers, Web extensions like ad- and tracker-blockers help users experience the Web on their own terms—against the best efforts of advertisers.

Policymakers can foster interoperability in two ways. First, we should help enable competitive compatibility (ComCom) by neutralizing the legal weapons that big companies use to lock down use of their products, which would pave the way for competitors to tinker and extend without fear of legal reprisal. Second, we support new interoperability mandates—data portability, back-end interoperability, and delegability—to guarantee accessible tools for interoperation.

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

3.1. Competitive Compatibility

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

ComCom is absolutely essential for innovation. Overwhelmingly, the technologies we rely on today were not established as full-blown, standalone products; rather, they started as adjuncts to the incumbent technologies that they eventually grew to eclipse.

The first cable TV service grew out of hobbyist efforts to bring big-city TV networks to their small-market towns. Modems were unsanctioned add-ons to Ma Bell's ubiquitous copper phone lines. Before the Web, a tool called Gopher defied network operators' intentions and made information from around the Internet accessible to the masses. Printers, ad-blockers, tape-deck audio jacks, and personal finance empires grew and thrived—not because anyone deliberately let them, but because nobody could stop them.

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

Unfortunately, some companies deploy a set of legal tools to undermine those rights and stave off small competitors, including the DMCA, CFAA, and Terms of Service and user agreements.

The **Digital Millennium Copyright Act (DMCA)** is the 1998 law that overhauled copyright in the digital world. It contains "anti-circumvention" provisions (section 1201) that bar circumvention of access controls and copy controls. This can be, and frequently is, used to shut down those who would devise new uses for their devices and services.

The **Computer Fraud and Abuse Act (CFAA)** is another law that has grown beyond its original purview, becoming a powerful way to restrict interoperation. The CFAA was intended to establish penalties for malicious hacking, but it's been misused to target all kinds of much more benign activities, including the creation of add-on products that depend on interoperability. The law provides civil and criminal penalties for one who "intentionally accesses a computer without authorization or exceeds authorized access." Overbroad interpretations of this clause attempt to equate compliance with the law to compliance with Terms of Service. This has given private companies across the country power to decide what is unlawful and who prosecutors can go after for alleged computer crimes.

Even outside the context of the CFAA, **Terms of Service (ToS)** and their cousins, **End User License Agreements (EULAs)**, can be used to limit interoperability. These contracts, associated with nearly every technology good or service on the market today, can be loaded with language forbidding reverse engineering and the use of add-on services that require interoperability. Manufacturers are unlikely to sue users who violate those terms, but they will enforce those terms against third-party interoperators who try to modify the customer experience.

All of these legal constructs are in need of serious reform. In several cases, that reform can begin without changing the statutes themselves.

For example, the DMCA already has language to protect innovators —courts just need to interpret it better. The DMCA contains a permanent exemption that allows you to circumvent a technological protection measure if it's necessary to analyze software to achieve interoperability, as long as that's your sole purpose in circumventing. But EFF is not aware of any case in which this carve-out was successful. A more complete protection for interoperability would be for courts to interpret Section 1201 of the DMCA to require a nexus to copyright infringement. In other words, only those whose circumvention is done in service of infringement would be breaking the law, while those doing noninfringing things, like analyzing code to make interoperable technology, would be free to do so.

The CFAA, too, can be better construed. A case now pending before the Supreme Court may help clarify that violating TOS is not a crime. In Van Buren v. United States, the Court will for the first time consider if the CFAA criminalizes access that simply violates the use restrictions or TOS that companies impose to control the use of their websites, apps, and computer systems. A broad array of organizations and trade associations, including EFF, have urged the Court to construe the CFAA to target only those who break into computer networks to sabotage them or steal sensitive data. If the Court does so, it will be a win for competition.

EULAs and ToS are non-negotiated contracts —"take it or leave it" arrangements, also called contracts of adhesion. Those "contracts" often include surprising terms that strip users of fundamental speech rights, and enforcing those contracts the same way we do with freely negotiated deals leads to shocking results. Fortunately, the law provides multiple independent bases to rein in such abusive policy practices: the "reasonable expectations" doctrine, unconscionability, and public policy limits on their enforcement. With a series of good rulings, abusive or highly anticompetitive ToS may be eradicated as a matter of legal precedent.

Outside the courtroom, we can and should promote ComCom by pressuring Congress to pass long-pending legislation to rebalance the CFAA and Section 1201 and bring them closer to their intended purpose. We can demand new federal legislation protecting digital first sale, and legislation at all levels protecting the right to repair. We can also ask our state representatives to declare that as a matter of public policy, their state favors contracts that support interoperability, just as some states reject noncompetitive employment contract terms. Each of these would help.

Finally, in addition to reining in laws that block interoperability, governments at every level can take steps to actively encourage it. The Open Source Definition is a framework for software licensing, designed to maximize certainty for new market entrants who make interoperable products and services; government procurement rules could dictate that only open source-friendly vendors will be considered. Consent decrees arising from FTC or other enforcement actions (including lawsuits) can impose behavioral remedies on bad-behaving companies, barring them from taking action against interoperators or requiring them to open their licensing terms. Voluntary covenants in standards bodies, professional associations, or federations (such as academic or research consortia) can bind adherents to standards of fair play. All of these can be used to make dominant companies more hospitable to interoperability.

Example 1: Giving communities the tools for self-determination

After years of Facebook selling its groups as resources for medical communities, those same communities have been victims of multiple serious defects in Facebook's group privacy model. In one notable example, the membership of a closed Facebook group of cancer "previvors" who carried a gene for breast cancer was in fact more broadly visible to third parties and marketers, effectively outing all of its members. The collective action problem of shifting the entire group to a rival platform was so pernicious that it carries on to this day.

Imagine if the group members had been able to use a community migration tool that set up a two-way, scrape-and-push link between a Diaspora pod and a Facebook group, appending messages with a footer that alerted users to the proportion of group members (or message volume) that had migrated off Facebook. Once a certain threshold was met (51%, 75%, etc), the Diaspora community could have automatically severed its link to Facebook.

This could be accomplished with ComCom: the technical tools required are straightforward, and could be built on top of Facebook's groups system. Such a measure allows partial connectivity between dominant platforms and new entrants—to keep hold of the vine they're swinging on until they have a firm grip on the next one—and to gradually transition from a dominant platform to an upstart platform, lowering transaction costs and solving collective action problems.

3.2. Interoperability Mandates[1]

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

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

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

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

3.2.1. Data portability

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

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

[1] By "mandates" here we refer to requirements that platforms take affirmative steps, where necessary, to ensure that users (and the companies that serve them) have these capabilities. We specifically are not, and indeed strongly discourage, mandates that require specific or similar specific steps for how such capabilities are to be achieved.

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

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

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

3.2.2. Back-end interoperability

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

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

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

Example 2: Federated social networking

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

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

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

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

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

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

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

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

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

3.2.3. Delegability

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

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

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

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

Example 3: Third-party privacy controls

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

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

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

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

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

4. Interoperability: Risks and Mitigations

Both competitive compatibility and platform-sanctioned interoperability create privacy risks for users. ComCom applications are often villainized by the platforms, sometimes with good reason. Any third-party application that puts itself between a user and a user interface, like a screen-scraping financial data aggregator or a browser extension, can see everything that the user can see. And they do not always take good care of what they collect. Yodlee, a financial data aggregator in the vein of Mint, sells its data to hedge funds; some browser extensions have features that look a lot like spyware.

The APIs that companies voluntarily expose are also abused, often dramatically. When Cambridge Analytica set out to build psychographic profiles on millions of voters, it was able to gather data from users and their friends without those friends' consent. Internal documents reveal that while the collection occurred, Facebook executives were already considering curtaining the access they offered to apps like Cambridge Analytica's thisisyourdigitallife. By the time the story broke, Facebook had long since shut down the offending APIs. But once the data got out, neither Facebook nor the users it exposed could do anything to bring it back.

Users rarely have legal recourse when their privacy is violated by an interoperator (a problem we would like to solve by enacting comprehensive consumer data privacy legislation, including a private right of action). The platforms, in contrast, now have several courses of action. If the offending party is using a sanctioned API or distributing an app through a company store, the platform can simply remove their privileges. The platform can also change the way a product works, either to reduce the privileges that API users enjoy or to foil an adversarial interoperator. In some cases, they may go as far as to sue the offending third party using claims under CFAA or copyright law.

In short: when interoperability happens, data gets shared, sometimes by design and sometimes in spite of it. When that data is misused, platforms may respond by removing the interoperability they choose to support or by using the law to shut it down.

All of this happens against the backdrop of a United States that is sorely lacking in national consumer privacy law. If consumer privacy were properly protected, these issues would not be nearly so pressing. Without a privacy regime, policymakers in the tech space must more carefully consider the consequences that every new policy may have on user privacy. What protections do exist are often brittle, cobbled together from accidental shared interests, and reliant on the whims of monopolists.

Change anything about the balance of power, some argue, and the whole system stands to collapse into chaos. This misses the point: it's already chaos. Privacy in the digital world is not okay. We need to fix the system with laws that actually address the problem, directly and with conviction. And a huge part of the problem is monopoly.

4.1. Competitive Compatibility

4.1.1. Risks of curtailing corporations' legal weapons

Currently, companies can use the DMCA, CFAA, contract law, and other legal theories to shut down ComCom interoperators. And large platforms sometimes use these theories to cut off access to actors that they say would violate user privacy.

The pro-privacy argument against ComCom falls along two lines:

1. Rational companies wield their exclusionary powers wisely: they act as proxies for their users' interests, blocking privacy-invaders, fraudsters, and other bad actors.
2. Legal rights to exclude are a cost-effective way to deter bad actors; one effective lawsuit brought by Facebook against Power Ventures chilled investment in the sector for a decade. To the extent that companies should exclude, legal tools are the best way to do so.

Understanding these arguments is key to understanding why ComCom-positive policy could create new risks for users. It's true that bad actors—like data brokers—are sometimes deterred by the legal instruments that we propose scaling back. However, the privacy issues that ComCom highlights are not inherent to the kinds of data sharing that ComCom will enable: they are results of the lack of adequate privacy protections in the United States.

First up is the idea that large, dominant Internet companies act as good stewards of their users' data. Market concentration and lax privacy and security regulation have created what Bruce Schneier calls "feudal security." Users—whose lives are increasingly digitized—do not have a public system that safeguards their security and safety, even as the consequences of breaches become more severe. Left without democratic institutions to defend their interests, users throw their lot in with "feudal" seigneurs, lordly mega-corporations that defend all those who pledge their fealty and put down roots in their demesne.

This system has real benefits to users, so long as their interests are coterminous with the interests of the companies they have entrusted: if you want to be defended against malicious apps, the iOS App Store will do a pretty good job of it. Of course, when your interests diverge from the company's (if you're a Uyghur hoping to have an effective VPN to use in China), then the seigneur's priorities take precedence over yours, with undesirable (and even lethal) consequences.

If anti-ComCom tools are removed, the argument goes, the seigneurs upon whose might many users depend will be weakened.

The platforms do, indeed, shut down interoperability in order to protect their users. Often, a platform can moderate its services by simply revoking API keys or pulling apps

from an app store. In these cases, the platform doesn't have to reach beyond its own walls, it just has to stop granting certain privileges. An affirmative right to ComCom generally won't stop companies from tending their own gardens in this way.

Platforms also do more than just moderate; they also expend design and engineering time to stop interoperators who don't ask permission. Sometimes this is done with targeted technical countermeasures, as in the age-old battle between virus and antivirus. Windows Defender and other antivirus programs check executable files for characteristics of known malware. They attempt to prevent specific behaviors that are known to have caused problems in the past. Sometimes, developers try to lock down a product so that nobody can do anything the seller doesn't intend, as Apple has done with nearly every part of its iOS ecosystem.

For example, one of the most common ComCom activities is "scraping," or automatically gathering data through a web interface. Scraping is used for constructive things all the time, from public-interest research to opening up new markets. But it's also a favored tool of data brokers. The huge amount of data made public via social media can be gathered by anyone with an Internet connection and some scripts. Dystopian trailblazer Clearview AI built a database of three billion faceprints, which it uses to assist police identify suspects, by scraping photos from social media.

Facebook is a frequent target of scraping, and uses the CFAA to fight it. Last year, the company filed a set of cases against companies that allegedly collected Facebook users' data through browser extensions. According to Facebook, this kind of legal action is rare. In its press release, the company claimed their action "marked one of the the first times a social media company used a coordinated legal strategy across jurisdictions to enforce its Terms and protect its users."

Facebook's statement, while true, is misleading. It's a mistake to confine the history of anti-interoperability gambits to legal cases that actually reach a courtroom. Often, the mere possibility of a lawsuit is enough to scare away would-be data gatherers. Companies deploy technical countermeasures as a first line of defense, but may count on a legal backstop if the levees break. Likewise, would-be interoperators know they need to get past a firm's technical restrictions, but they also know that doing so might only win them a date in court at the defendant's table.

Removing this legal backstop would fundamentally change the balance of power. It would create a space for both investments and unabashed, concerted, cooperative efforts to defeat technical countermeasures that incumbents prop up. It could tip the scales against the platforms, despite their budgets for technical expertise, and might usher in a new wave of follow-on innovation.

A more ComCom-positive legal regime would mean Facebook can't bring CFAA charges against data brokers simply for scraping, or block extensions that collect Facebook user data. Is this an acceptable tradeoff?

4.1.2. Mitigating privacy and security risks

First, companies are good custodians of their users' privacy only to the extent that this is a profitable strategy. App store moderation can protect users from abuse, but as with Android's ban on ad-blockers and iOS's Chinese ban on VPNs, moderation can also undermine privacy. Google balances privacy protection with tracking-derived revenues, and Apple balances privacy protection with access to Chinese manufacturing and customers.

The anti-ComCom laws we propose narrowing are designed to protect companies from hackers, copyright infringement, and other threats to their bottom line—and companies have no obligation to deploy lawyers on their users' behalf. Monopolists have little incentive to engage in costly lawsuits against third-party privacy violators unless user outrage reaches a critical mass. As a result, companies have rarely used the laws we're concerned with to defend users, unless they're also defending their own shareholders.

Second, it's worth reiterating that nothing about removing legal barriers to competitive compatibility will impose new restrictions on what technical countermeasures platforms can deploy in defense of their users. Companies that are subject to technical mandates may be required to work with competitors they would otherwise have blocked, but ComCom-related policy will not stop platforms from trying to out-engineer their rivals.

Third, even when companies do want to sue to protect their users, they lack the right tools to do so. Privacy should be protected by privacy laws, not copyright law and CFAA. Even when companies want to do the right thing, lawsuits against bad actors can make bad law. Criminalizing Web scraping and ToS violations (which are not usually associated with more serious security breaches) does far more harm than good. We would do better to develop and implement targeted privacy protections, rather than perverting computer crime law far beyond its intended purpose.

Finally, ComCom would create space for new, better privacy protections and tools. Platform seigneurs have historically done more harm than good for user privacy, and the few examples of monopolists' interests aligning with their users' are not enough to justify the status quo. In the absence of other changes to law, we believe that competitive compatibility will not lead to significant new privacy issues for users. On the contrary, it will license users and third parties to develop add-ons, like the privacy settings manager in Example 3, that modify services to be more privacy-preserving. And as discussed in Example 1, when a platform doesn't live up to their promises, it could help users execute a coordinate exodus to a competitor.

The ability of rival competitors (or co-ops, or tinkerers) to allow users to override these dominant actors' choices creates the possibility of a dynamic, evolving market, where new products rise to the fore on the basis of quality, rather than inertia or lock-in. More importantly, it allows users whose privacy needs are not compatible with a manufacturer's commercial priorities to bypass the manufacturer's decisions.

In our analysis, the most significant privacy harm that could be exacerbated by these proposals is the collection of potentially sensitive data from publicly-available websites by data brokers and other snoops. This is a problem, but it's only the tip of a massive, severely underregulated iceberg of an industry. Even when data brokers collect personal information from Facebook, the most significant privacy harm does not happen at the point of collection, it happens during the subsequent processing and exploitation of the data. We would do better to develop and implement targeted privacy protections, rather than perverting computer crime law far beyond its intended purpose. Relying on Facebook's use of CFAA to regulate these actors is like hoping bank robbers get pulled over for speeding in their getaway car.

Ultimately, ComCom represents a trade-off: users whose privacy interests are well-protected by vendors will find their defenders with fewer legal weapons and more dependent on technical ones. But the worst actors—deliberate criminals—already violate the law to get at user data, and so companies can't be wholly dependent on the law in any event. Meanwhile, users whose privacy interests diverge from corporate platforms' priorities will have new options to protect themselves. And, finally, the platforms themselves will face marketplace retaliation for abusing user privacy, because users will find it easier than ever to shop around for better privacy without having to sacrifice their enjoyment of bad privacy actors' services.

4.2. Interoperability Mandates

Requiring platforms to share more data may appear to go against trends in both privacy law and platform development in the past few years. GDPR, CCPA, and other privacy laws have put new restrictions that target the movement of personal data between platforms. And over the past half-decade, Facebook, Twitter, and others have mostly restricted, not expanded, their public-facing APIs. In the long shadow of Facebook's Cambridge Analytica scandal, it is reasonable to be suspicious of new pathways for user data.

But that's precisely why we need new rules of engagement: to counter the anticompetitive and privacy-invasive effects of personal data concentrating in a few hands, while ensuring that any data that is shared is bound by strong restrictions on minimization and consent. In this section, we discuss the new risks interoperability mandates pose to privacy and security, and how we can mitigate them.

4.2.1. Data portability

While portability is simpler to imagine and to implement than the other mandates we discuss, it still comes with risks. Furthermore, portability mandates apply to companies of all sizes, so the risks must be considered in the context of small startups and companies outside of the traditional tech sector.

Security and privacy risks

Unlike policies to facilitate competitive compatibility, portability mandates require businesses to intentionally create new channels for sharing data. In some cases, existing

portability laws also stipulate that portable data must be easy to access: that is, users should not have to go through a lengthy verification process in order to receive their data. But if it's too easy—if a company doesn't properly verify that a user is who they say they are—then it can be easy for thieves to get it, too.

This has already proven to be an issue for companies implementing GDPR. Researchers have shown that many companies are too lax with their verification, making it easy for bad actors to access sensitive data that belongs to others. This is a real problem.

Portability mandates could also create ways to access data that didn't exist before. Generally, data portability mandates cause companies to create a single portal where all of a user's data can be accessed at once. This, in turn, could create new targets for phishing or other kinds of credential theft.

Finally, it may be difficult to determine which data is subject to access requests from which people. In the past, Facebook has claimed that it cannot simply allow users to download a portable version of their friends list (complete with email addresses and phone numbers, if public), because their friends might not want Facebook to share their contact information. As a result, it created separate settings for making one's contact information searchable and viewable by friends, and for allowing one's friends to download that information as part of a data export. It made the export setting opt-in. The good-faith argument for this practice is that allowing programmatic access to certain data introduces privacy risks that are distinct from allowing a user to read or search for that same data by hand. Of course, granting automated access to friends' contact information would also be a direct threat to Facebook's ability to prevent competitors from gaining a foothold.

Mitigations

Some risks of portability are exaggerated, and do not need specific mitigation. For example, the idea that access to specific data via portability is materially riskier than access via a GUI is misguided. If a user has rightful, consensual access to others' data—whether or not it's directly about themselves—they should be able to access it the way they want. If granting users the right to export data they can already access creates substantial privacy risks, perhaps that data shouldn't be available to them in the first place. Letting a user "see" a piece of information but not "download" it is rarely an effective privacy control—but it is a stubborn roadblock to smooth data portability.

More difficult is making sure that exported data goes where it should. Some companies, especially large ones, already have sophisticated means of identifying their users and sharing sensitive data with them. However, a portability rule applied to all companies that handle user data will include a lot of businesses that don't currently have secure ways of identifying people. There's no easy way to guarantee that a person exercising the right to portability is who they say they are, but thoughtful regulation can go a long way. The California Consumer Privacy Act required rulemaking about Californians' new "right to know," a version of a right to data portability. EFF submitted comments to the California Attorney General, recommending that the AG give specific guidance for companies in some situations, but leave leeway for corner cases, such as when a user

doesn't have an account with a business and isn't identified by a legal identifier. Obvious safeguards against bad corporate behavior should apply here too: for example, any information that a user shares for the sake of verifying themselves should only be used for that purpose.

A user should be able to exercise their right to portability, and doing so should be simple whenever possible. At the same time, businesses should have discretion to deny access when a user truly can't be identified, especially if sensitive information is at stake. A regulatory body, in this case the California AG, has the ability to review cases where a user feels they've been denied their rights.

This style of mandate gives businesses incentives on two sides. First, if a business is found to be willfully and unfairly denying a user's right to port their data, it can suffer penalties. On the other hand, it can also be found liable if it recklessly shares a user's information with the wrong person. The sum of these incentives means that businesses should want to do what is best for users: share their data when they ask, whenever that's possible without excessive risk.

4.2.2. Back-end interoperability and delegability

Interoperability mandates for both the server-side ("back-end interoperability") and the client-side ("delegability") require large companies to open up new data flows to smaller interoperators. These pipelines should be able to achieve their objectives—of increasing competition, innovation, and user choice—without subjecting users to new risks or bolstering the surveillance business model.

Security and privacy risks

The security and privacy risks of back-end interoperability and delegability mandates fall into three categories:

1. Data sharing and mining via new APIs;
2. New opportunities for phishing and sock puppetry in a federated ecosystem; and
3. More friction for platforms trying to maintain a secure system.

The fact that new data will flow across company boundaries is not the only source of risk. We also need to consider the consequences of breaking up a centralized platform's power via federation, and of introducing government oversight to a fast-moving industry where security matters.

Data sharing and data mining

As described in Example 2, in order to enable federation, Facebook would need to create a new set of interfaces that allow competitors to jack in and connect users across the borders of the company. Services that use these will have access to very sensitive data about the people they are connecting and will need to be prepared to protect it.

This type of interoperation will expose huge amounts of behavioral data on users. Of course, Facebook and many other platforms already do this through their APIs and ad

networks, though the platforms reserve the right to revoke any company's access for nearly any reason. Interoperability mandates would take decisions about who gets access to what out of the platforms' hands, to a degree.

Without new legal safeguards to protect the privacy of user data, this kind of interoperable ecosystem could make Cambridge Analytica-style attacks more common. Smaller social media servers might try to build a business around passively profiling users of other services they federate with. Cambridge Analytica's entree to Facebook data was through an app downloaded by just over a quarter of a million people, a paltry number in social media circles. Any federated server that hosted a similar number of users could have access to all the same information that the Cambridge Analytica app thisisyourdigitallife had, plus much more.

Even when smaller services act honestly, interoperating can be difficult, and there is a risk that user data will be mishandled in the shuffle. Privacy settings for social networks like Facebook are more complex than "share" or "don't share." To match user expectations, platforms that federate with Facebook will need to respect those settings in all their subtleties. If they do not (or cannot) match those settings, it could lead to data being shared beyond what users anticipate and being used in ways they don't expect.

Delegability carries similar risks. Facebook's first attempts at client-side interfaces, including parts of the infamous early Graph API, were also nightmares for privacy. The problem was not necessarily that third-party tools could access lots of user data; that's a prerequisite for any user-level API. The problem was that users didn't understand who was accessing what, and Facebook did not police what companies were doing with data after they got it.

Web extensions are also an instructive example. They enable ComCom at the website level, but extensions are also built on powerful APIs that give direct access to the browser. These APIs can be used for good or ill. The WebExtension API powers some of the most innovative and user-positive tools on the Internet, from ad- and tracker-blockers to accessibility helpers to archivers to transparency tools. But it has also allowed hundreds of companies to harvest and sell sensitive information from unsuspecting users. We have explained elsewhere that Google's Chrome browser cannot roll back most of the extension APIs that allow harm without also nerfing tracker blockers; there will be similar tensions with most other delegable interfaces one could imagine.

Imagine an alternate Facebook Newsfeed plug-in that lets you set the rules for what content shows up on your feed and how. The plug-in will see everything you see, and potentially even more things—like metadata, or filtered content—that you cannot readily access. Any user who partners with a delegated agent will likely expose a lot of data to that agent or their code. But delegated agents will have access to data from many different users, not just the ones who choose to use their services. Sharing a post with "friends" will also mean sharing with "friends and their delegated agents."

This problem is similar to the issue we explored with data portability above: the privacy risks that can arise from giving automated access to information that users already have "manual" access to. However, it's one thing when portability a user has the power to download their own data; it's another when delegability gives a third-party company proxy access to data from thousands. One user is unlikely to develop invasive profiles on their own friends, but a third-party delegate may want to use its users' positions in a social network to do so. When thousands of Facebook users installed thisisyourdigitallife, the trojan horse app that gathered data from Cambridge Analytica's psychographic profiling, it had access to the "likes" of each user's friends. That alone was enough to kick off a huge privacy scandal, leading to the biggest fine in Federal Trade Commission history. Delegated agents will have access to everything, instantly and continuously.

Ultimately, this kind of access is necessary for the dream of delegability to work. As a result, privacy issues will have to be addressed at the policy level, with new privacy laws and safeguards on new interfaces. We discuss these safeguards in depth in the next section.

Phishing and sock puppetry

Of course, not everyone works within the bounds of the law. A second risk is that these mandates could expand the attack surface for criminal enterprises and state actors who are not afraid to be unfair and deceptive. In theory, a bad actor could spin up a federated social media server (or compromise an existing one), create a legion of fake identities, and send "friend requests" to thousands of different users in a phishing expedition. Less dramatically, bad actors may learn that a part of the federated ecosystem —perhaps a single server with little funding or poor security practices —is more amenable to users who would present false fronts to the rest of the world, and use that service as a base for their bad-faith operations. This is similar to the way that phishers and law enforcement "sock puppets" already abuse social media, but a given platform would have less power to shut down users on other federated services.

Security and vulnerability patching

Finally, it's worth giving special consideration to interoperable interfaces that require sophisticated security. For example, consider an interoperable, end-to-end encrypted messaging service. If we require the maintainer of such a service to present stable interfaces, and make it difficult for them to update or change those interfaces, it might become harder for them to keep their service secure. A poorly structured mandate could force companies to compromise or drag their feet on security, and this could undermine some of the progress made with end-to-end encrypted services in walled gardens.

Mitigations

Even with all of these risks, a well-crafted interoperability mandate should be a net benefit for privacy. Architects of new interoperability policy will have the opportunity to establish guardrails on the specific data-sharing pathways that policy creates.

Moreover, under the proposed regime, only a small number of large companies would be required to open up new sets of interfaces, which should be easier to monitor than an industry wide change. And where platforms' incentives align with users', such as in the battle against phishing and the continual quest for sound cryptography, the best approach may be to get out of the way.

Preventing personal data abuse

We need clear rules and protections to ensure that platform interfaces meet interoperability requirements while protecting the data that flows across those interfaces. This goes for both client-side interfaces (created for delegability) and back-end interfaces (for federation). Neither the platforms subject to new requirements nor the companies that interoperate with them should collect more data than necessary for the purposes of interoperability. Neither party should be allowed to monetize or exploit the data they collect for secondary purposes. And both parties should verify that they have a user's informed consent before beginning to transfer personal data across such an interface.

Two principles must guide privacy rules: minimization and consent. Together, they can help ensure user autonomy to control their own use of technology.

First, privacy rules must require minimization of the processing of users' data, including collection, retention, sharing, and use. Interoperability will require that platforms share lots of data, but companies that interoperate with regulated platforms must be barred from processing any more of a user's data than is strictly necessary to give them what they asked for. The platforms themselves will define the interfaces, and their incentives should naturally be aligned towards user privacy: they won't want to share any more data than they need to. Not so for third-party services which choose to federate via the newly created interfaces: these may be inclined to process as much data as they can, and be tempted to use data in ways users may not want. Thus, strong legal safeguards are needed to ensure that when a user decides to link up with a friend on a new service, their data is only used in ways they expect.

Second, privacy rules must require informed opt-in consent. Users must be given a choice whether or not to start interacting with another platform, and must be able to withdraw consent at any time. At every stage, users must be made aware of what data they are sharing with whom, why that data must be shared, and what it will be used for. In the case of back-end interfaces, the platform should be responsible for informing a user and obtaining their actual, informed consent. In the case of client-side interfaces to satisfy delegability mandates, the companies that act as delegated agents should bear the burden of notice and consent, and be held responsible when they act badly.

Both consent and minimization rules are necessary. Absent a minimization requirement, companies that profit from surveillance are skilled at deploying dark patterns to manufacture phony "consent." Additionally, certain uses of data collected through these legally-mandated interfaces should be absolutely off-limits, such as selling it to third parties or monetizing it through targeted ads.

Absent a consent requirement, a minimization rule might not adequately reflect the interests of individual users either. There is no one-size-fits-all approach to privacy, and there will be situations in which users deserve to make choices about how their data are collected and processed.

Once again, consider the fully federated social network from Example 2. When building back-end interfaces for federating its service, Facebook will need to make sure it shares only the content that users direct it to share. But once PII crosses that threshold, it's up to the receiving service to handle that information properly. Social media users in a federated ecosystem will likely think about data sharing in terms of which people will have access to it—not which companies. When sending a text message, one does not usually think about which carrier will receive it or what they will do with it. And that is how it should be.

That means services in a federated network must abide by a consistent set of policies with respect to data that is shared across their boundaries. Where the policies of two services clash, it should be the responsibility of the satellite service—the one which is choosing to federate with a regulated platform—to make sure it handles the data it receives from the platform in the right way. On the other side, a platform that does share its users' data through such an interface must make sure federated partners have all the information they need to process personal information according to each user's preferences.

Addressing identity, phishing, and security

As we discussed, back-end interoperability and federation may exacerbate extant classes of attacks on user privacy, like phishing or sock puppetry. One way to mitigate this danger is with more stringent identity verification, so that users anywhere in the federated social media ecosystem can have confidence that they know who they are talking to. However, identity verification is a privacy issue of its own. Facebook is notorious for its intrusive and harmful "real names" or "authentic names" policy. Modern data brokers make millions in the identity verification business, hawking location, behavioral data, and other personal information so that businesses can be sure a customer is who they say they are.

Interoperability brings this tension between verification and anonymity to the fore, but doesn't necessarily worsen it. In a world where users can interact with each other across services, they should be able to make an informed choice about whether to trust a message from a Facebook-verified "authentic name" or a user identified by email address on a small, volunteer-run server. In fact, one of the biggest benefits of a federated social networking ecosystem will be that users who have been unfairly banned by Facebook, or who have simply chosen to abstain, can get in touch with their friends and family who do use the platform.

Simple design choices, like asking a user to accept an invitation to a conversation before they can receive unsolicited messages, go a long way towards mitigating phishing and spam. It is also worth noting that social media platforms currently have incentives to encourage as many connections between their users as possible, and are constantly

suggesting new "friends" or "connections;" reducing those incentives might lead the platforms to develop user interfaces that are not so bent on proliferating network connections. Expertise and tools to detect malicious communications, which were largely either bought up or developed in-house by the larger platforms in the last decade, could instead find other customers as a more general third-party service for end-users or a market of smaller interoperable competitors.

Adding it all together: Law, code, and competition

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

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

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

5. Conclusion

The problems of corporate concentration and privacy on the Internet are inextricably linked. We believe that a new regime of interoperability can revitalize competition, encourage innovation, and give users more self-determination in their digital lives. It's natural to imagine that new, legally-protected or legally-mandated data flows will lead to new privacy and security risks. But as we've shown, those risks are not as grave as they might first appear, and they can be mitigated. A more interoperable Internet can and should be a more private one.

New interoperability mandates will create new data flows, and will take some discretion out of the hands of the platforms. Facebook and Google may be forced to share personal information with companies they wouldn't have before. But mandates can come with strings attached, in the form of legal obligations for informed consent and data minimization. As a result, data that flows across these new interfaces may be more legally protected than any data that the platforms have chosen to share in the past.

Creating more space for competitive compatibility will free tinkerers, startups, and nonprofits to interact with big platforms in ways that the platforms might not approve of—or might not have imagined. Will removing tools incumbents use to shut down ComCom hinder the platforms' ability to protect their users? We do not believe so. It's true that companies can sometimes use non-privacy laws to shield their users from legitimate privacy threats. But these legal tools have never been properly calibrated to protect users.

In general, objections to interoperability presume that the companies who hold user data are best positioned to protect it. This is sometimes the case, but too often, the incentives of a platform and its users do not align. In the past, companies have often chosen to interoperate in ways that make them money at the expense of privacy—consider the ad tech ecosystem, in which millions of websites and apps interoperate with Google, Facebook, Amazon, and other ad platforms, swapping personal data and screen real estate for fractions of a penny per impression. The same companies have also refused to interoperate in ways their users might want when interoperation would mean sacrificing a competitive advantage. Clearly, when companies decide whether to share data, user welfare is not always the first concern.

More than anything, the dangers of data-sharing that we have addressed here underline the need for better privacy law. In a world where user consent and purpose minimization are properly defined and vigorously protected, most of the concerns with new interoperability programs would be moot. More importantly, the idea that we must rely on platforms' good will for our protection would seem rightfully absurd. EFF will continue to fight for better privacy laws. Towards that end, we believe interoperability and other pro-competitive policies are critical to breaking the platforms' plutocratic influence over lawmakers. And we believe a more interoperable Internet will be more innovative, less concentrated, and more amenable to user rights.

6. Appendix: The GDPR, Privacy and Monopoly

In Privacy Without Monopoly: Data Protection and Interoperability, we took a thorough look at the privacy implications of various kinds of interoperability. We examined the potential privacy risks of interoperability mandates, such as those contemplated by 2020's ACCESS Act (USA), the Digital Services Act and Digital Markets Act (EU), and the recommendations presented in the Competition and Markets Authority report on online markets and digital advertising (UK).

We also looked at the privacy implications of "competitive compatibility" (comcom, AKA adversarial interoperability), where new services are able to interoperate with existing incumbents without their permission, by using reverse-engineering, bots, scraping, and other improvised techniques common to unsanctioned innovation.

Our analysis concluded that while **interoperability created new privacy risks** (for example, that a new firm might misappropriate user data under cover of helping users move from a dominant service to a new rival), these risks can largely be mitigated with thoughtful regulation and strong enforcement. More importantly, **interoperability also had new privacy benefits**, both because it made it easier to leave a service with unsuitable privacy policies, and because this created real costs for dominant firms that did not respect their users' privacy: namely, an easy way for those users to make their displeasure known by leaving the service.

Critics of interoperability (including the dominant firms targeted by interoperability proposals) emphasize the fact that weakening a tech platform's ability to control its users weakens its power to defend its users.

They're not wrong, but they're not complete either. It's fine for companies to defend their users' privacy—we should accept nothing less—but the standards for defending user-privacy shouldn't be set by corporate fiat in a remote boardroom, they should come from democratically accountable law and regulation.

The United States lags in this regard: Americans whose privacy is violated have to rely on patchy (and often absent) state privacy laws. The country needs—and deserves—a strong federal privacy law with a private right of action.

That's something Europeans actually have. The General Data Protection Regulation (GDPR), a powerful, far-reaching, and comprehensive (if flawed and sometimes frustrating) privacy law came into effect in 2018.

The European Commission's pending Digital Services Act (DSA) and Digital Markets Act (DMA) both contemplate some degree of interoperability, prompting two questions:

1. Does the GDPR mean that the EU doesn't need interoperability in order to protect Europeans' privacy? And
2. Does the GDPR mean that interoperability is impossible, because there is no way to satisfy data protection requirements while permitting third-party access to an online service?

We think the answers are "no" and "no," respectively. Below, we explain why.

6.1 Does the GDPR mean that the EU doesn't need interoperability in order to protect Europeans' privacy?

Increased interoperability can help to address user lock-in and ultimately create opportunities for services to offer better data protection.

The European Data Protection Supervisor has weighed in on the relation between the GDPR and the Digital Markets Act (DMA), and they affirmed that interoperability can advance the GDPR's goals.

Note that the GDPR doesn't directly mandate interoperability, but rather "data portability," the ability to take your data from one online service to another. In this regard, the GDPR represents the first two steps of a three-step process for full technological self-determination:

1. The right to access your data, and
2. The right to take your data somewhere else.

The GDPR's data portability framework is an important start! Lawmakers correctly identified the potential of data portability to help promote competition of platform services and to reduce the risk of user lock-in by reducing switching costs for users.

The law is clear on the duty of platforms to provide data in a structured, commonly used and machine-readable format and users should have the right to transmit data without hindrance from one data controller to another. Where technically feasible, users also have the right to ask the data controller to transmit the data to another controller.

Recital 68 of the GDPR explains that *data controllers should be encouraged to develop interoperable formats that enable data portability.* The WP29, a former official European data protection advisory body, explained that this could be implemented by making application programme interfaces (APIs) available.

However, the GDPR's data portability limits and interoperability shortcomings have become more obvious since it came into effect. These shortcomings are exacerbated by

lax enforcement[2]. Data portability rights are insufficient to get Europeans the technological self-determination the GDPR seeks to achieve.

The limits the GDPR places on which data you have the right to export, and when you can demand that export, have not served their purpose. They have left users with a right to data portability, but few options about where to port that data to.

Missing from the GDPR is step three:

3. The right to interoperate with the service you just left.

The DMA proposal is a legislative way of filling in that missing third step, creating a "real time data portability" obligation, which is a step toward real interop, of the sort that will allow you to leave a service, but remain in contact with the users who stayed behind. An interop mandate breathes life into the moribund idea of data-portability.

6.2 Does the GDPR mean that interoperability is impossible, because there is no way to satisfy data protection requirements while permitting third-party access to an online service?

The GDPR is very far-reaching, and European officials are still coming to grips with its implications. It's conceivable that the Commission could propose a regulation that cannot be reconciled with EU data protection rules. We learned that in 2019, when the EU Parliament adopted the Copyright Directive without striking down the controversial and ill-conceived Article 13 (now Article 17). Article 17's proponents confidently asserted that it would result in mandatory copyright filters for all major online platforms, not realizing that those filters cannot be reconciled with the GDPR.

But we don't think that's what's going on here. Interoperability—both the narrow interop contemplated in the DMA, and more ambitious forms of interop beyond the conservative approach the Commission is taking—is fully compatible with European data protection, both in terms of what Europeans legitimately expect and what the GDPR guarantees.

Indeed, the existence of the GDPR *solves* the thorniest problem involved in interop and privacy. By establishing the rules for how providers must treat different types of data and when and how consent must be obtained and from whom during the construction

[2] noyb.eu: https://noyb.eu/en/statement-3rd-anniversary-gdpr, EP Resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 - Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18 (2020/2789(RSP)) https://www.europarl.europa.eu/doceo/document/exp.pdf

and operation of an interoperable service, the GDPR moves hard calls out of the corporate boardroom and into a democratic and accountable realm.

Facebook often asserts that its duty to other users means that it has to block you from bringing some of "your" data with you if you want to leave for a rival service. There is definitely some material on Facebook that is not yours, like private conversations between two or more other people. Even if you could figure out how to access those conversations, we want Facebook to take steps to block your access and prevent you from taking that data elsewhere.

But what about when Facebook asserts that its privacy duties mean it can't let you bring the replies to your private messages; or the comments on your public posts; or the entries in your address book; with you to a rival service? These are less clear-cut than the case of other peoples' private conversations, but blocking you from accessing this data also helps Facebook lock you onto its platform, which is also one of the most surveilled environments in the history of data-collection.

There's something genuinely perverse about vesting these calls with the reigning world champions of digital surveillance, especially because an unfavorable ruling about which data you can legitimately take with you when you leave Facebook might leave you stuck on Facebook, without a ready means to address any privacy concerns you have about Facebook's policies.

This is where the GDPR comes in. Rather than asking whether *Facebook* thinks you have the right to take certain data with you or to continue accessing that data from a rival platform, the GDPR lets us ask the *law* which kinds of data connections are legitimate, and when consent from other implicated users is warranted. Regulation can make good, accountable decisions about whether a survey app deserves access to all of the "likes" by all of its users' friends (Facebook decided it did, and the data ended up in the hands of Cambridge Analytica), or whether a user should be able to download a portable list of their friends to help switch to another service (which Facebook continues to prevent).

The point of an interoperability mandate—either the modest version in the DMA or a more robust version that allows full interop—is to allow alternatives to high-surveillance environments like Facebook to thrive by reducing switching costs. There's a hard collective action problem of getting all your friends to leave Facebook at the same time as you. If people can leave Facebook but stay in touch with their Facebook friends, they don't need to wait for everyone else in their social circle to feel the same way. They can leave today.

In a world where platforms—giants, startups, co-ops, nonprofits, tinkerers' hobbies—all treat the GDPR as the baseline for data-processing, services can differentiate themselves by going *beyond* the GDPR, sparking a race to the top for user privacy.

6.2.1 Consent, Minimization and Security

We can divide all the data that can be passed from a dominant platform to a new, interoperable rival into several categories. There is data that should not be passed. For example, a private conversation between two or more parties who do not want to leave the service and who have no connection to the new service. There is data that should be passed after a simple request from the user. For example, your own photos that you uploaded, with your own annotations; your own private and public messages, etc. Then there is data generated by others about you, such as ratings. Finally, there is someone else's personal information contained in a reply to a message you posted.

The last category is tricky, and it turns on the GDPR's very fulcrum: *consent*. The GDPR's rules on data portability clarify that exporting data needs to respect the rights and freedom of others. Thus, although there is no ban on porting data that does not belong to the requesting user, data from other users shouldn't be passed on without their explicit consent, or under another GDPR legal basis, and without further safeguards.

That poses a unique challenge for allowing users to take their data with them to other platforms, when that data implicates other users—but it also promises a unique benefit to those other users.

If the data you take with you to another platform implicates other users, the GDPR requires that they consent to it. The GDPR's rules for this are complex, but also flexible.

For example, say, in the future, that Facebook obtains consent from users to allow their friends to take the comments, annotations, and messages they send to those friends with them to new services. If you quit Facebook and take your data (including your friends' contributions to it) to a new service, the service doesn't have to bother all your friends to get their consent again—under the WP Guidelines, so long as the new service uses the data in a way that is consistent with the uses Facebook obtained consent for in the first place, that consent carries over.

But even though the new service doesn't have to obtain consent from your friends, it *does* have to notify them within 30 days - so your friends will always know where their data ended up.

And the new platform has all the same GDPR obligations that Facebook has: they must only process data when they have a "lawful basis" to do so; they must practice data minimization; they must maintain the confidentiality and security of the data; and they must be accountable for its use.

None of that prevents a new service from asking your friends for consent when you bring their data along with you from Facebook. A new service might decide to do this just to be sure that they are satisfying the "lawfulness" obligations under the GDPR.

One way to obtain that consent is to incorporate it into Facebook's own consent "onboarding"—the consent Facebook obtains when each user creates their account. To comply with the GDPR, Facebook already has to obtain consent for a broad range of data-processing activities. If Facebook were legally required to permit interoperability, it could amend its onboarding process to include consent for the additional uses involved in interop.

Of course, the GDPR does not permit far-reaching, speculative consent. There will be cases where no amount of onboarding consent can satisfy either the GDPR or the legitimate privacy expectations of users. In these cases, Facebook can serve as a "consent conduit," through which consent to allow their friends to take data with muddled claims with them to a rival platform can be sought, obtained, or declined.

Such a system would mean that some people who leave Facebook would have to abandon some of the data they'd hope to take with them—their friends' contact details, say, or the replies to a thread they started—and it would also mean that users who stayed behind would face a certain amount of administrative burden when their friends tried to leave the service. Facebook might dislike this on the grounds that it "degraded the user experience," but on the other hand, a flurry of notices from friends and family who are leaving Facebook behind might spur the users who stayed to reconsider that decision and leave as well.

For users pondering whether to allow their friends to take their blended data with them onto a new platform, the GDPR presents a vital assurance: because the GDPR does not permit companies to seek speculative, blanket consent for future activities for new purposes that you haven't already consented to, and because the companies your friends take your data to have no way of contacting you, they generally *cannot* lawfully make any further use of that data (except through one of the other narrow bases permitted by GDPR, for example, to fulfil a "legitimate interest") . Your friends can still access it, but neither they, nor the services they've fled to, can process your data beyond the scope of the initial consent to move it to the new context. Once the data and you are separated, there is no way for third parties to obtain the consent they'd need to lawfully repurpose it for new products or services.

Beyond consent, the GDPR binds online services to two other vital obligations: "data minimization" and "data security." These two requirements act as a further backstop to users whose data travels with their friends to a new platform.

Data minimization means that any user data that lands on a new platform has to be strictly necessary for its users' purposes (whether or not there might be some commercial reason to retain it). That means that if a Facebook rival imports your comments to its new user's posts, any irrelevant data that Facebook transmits along with that data (say, your location when you left the comment, or which link brought you to the post), must be discarded. This provides a second layer of protection for users whose friends migrate to new services: not only is their consent required before their blended data travels to the new service, but that service must not retain or process any extraneous information that seeps in along the way.

The GDPR's security guarantee, meanwhile, guards against improper handling of the data you consent to let your friends take with them to new services. That means that the data in transit has to be encrypted, and likewise the data at rest, on the rival service's servers. And no matter that the new service is a startup, it has a regulated, affirmative duty to practice good security across the board, with real liability if it commits a material omission that leads to a breach.

Without interoperability, the monopolistic high-surveillance platforms are likely to enjoy long term, sturdy dominance. The collective action problem represented by getting all the people on Facebook whose company you enjoy to leave at the same time you do means that anyone who leaves Facebook incurs a high switching cost.

Interoperability allows users to depart Facebook for rival platforms, including those that both honor the GDPR and go beyond its requirements. These smaller firms will have less political and economic influence than the monopolists whose dominance they erode, and when they do go wrong, their errors will be less consequential because they impact fewer users.

Without interoperability, privacy's best hope is to gentle Facebook, rendering it biddable and forcing it to abandon its deeply held beliefs in enrichment through nonconsensual surveillance —and to do all of this without the threat of an effective competitor that Facebook users can flee to no matter how badly it treats them.

Interoperability without privacy safeguards is a potential disaster, provoking a competition to see who can extract the most data from users while offering the least benefit in return. Every legislative and regulatory interoperability proposal in the US, the UK, and the EU contains some kind of privacy consideration, but the EU alone has a region-wide, strong privacy regulation that creates a consistent standard for data-protection no matter what measure is being contemplated. Having both components - an interoperability requirement and a comprehensive privacy regulation - is the best way to ensure interoperability leads to competition in desirable activities, not privacy invasions.