Ethics and Information Technology (2026) 28:15
https://doi.org/10.1007/s10676-026-09890-5

ORIGINAL PAPER

A Trade-off worth making: internet fragmentation and digital sovereignty

Scott Robbins[1]

Abstract
Opponents of digital sovereignty characterize the methods to achieve it as authoritarian, protectionist, and anti-innovation – ultimately leading to digital fragmentation. Digital fragmentation, roughly, is the idea that "the internet is in some danger of splintering into loosely coupled islands of connectivity." The internet is built on, so the argument goes, the foundation of open accessibility, free movement of data and interoperability. The exercise of digital sovereignty, it is claimed, chips away at this foundation – and threatens to fragment the internet as we know it. The argument against digital sovereignty is largely premised on an assumption that is in no way obviously true: the way the internet is benefits individuals. The current functioning of internet services requires consumers to give up large amounts of sensitive personal information that are used to generate targeted advertisements. These targeted advertisements have been associated with election tampering as well as a driving force in the dissemination of conspiracy theories leading to genocide, an armed insurrection, and making it much more difficult to get the world vaccinated. Opponents of digital sovereignty may be correct in their analysis that, in the current context, methods to achieve it will cause the internet to somewhat fragment. However, too often these opponents seem to defend a status quo that is fundamentally broken and dominated by a few companies which have time and again abused their power. Until the world agrees upon rules which protect privacy and ensure the functioning of democracy, the states must accept the trade of a fragmented internet for the protection of their citizens.

Keywords Internet Ethics · Data Localization · Internet Framentation · Surveillance Capitalism · Digial Sovereignty

Introduction

Opponents of digital sovereignty characterize the methods to achieve it as authoritarian, protectionist, and anti-innovation – ultimately leading to digital fragmentation (Accenture, 2017; Chander & Le, 2014; Cohen et al., 2017; Huddleston & Varas, 2020; Taylor, 2020). Digital fragmentation, roughly, is the idea that "the internet is in some danger of splintering into loosely coupled islands of connectivity" (Drake et al., 2016, p. 7). The internet is built on, so the argument goes, the foundation of open accessibility, free movement of data, and interoperability. The exercise of digital sovereignty, it is claimed, chips away at this foundation – and threatens to fragment the internet as we know it. Digital sovereignty can roughly be defined as state's 'control of data, software, standards and protocols, processes, hardware, services, and infrastructures' that make up the digital (Floridi, 2020, pp. 370–371). The argument against digital sovereignty is roughly that if states use some method X to obtain digital sovereignty, then digital fragmentation will occur. The fact that digital fragmentation is a bad thing that must be avoided is typically taken for granted (Accenture, 2017; EY Consulting, n.d.; Mueller, 2022, 2020).

The argument against digital sovereignty is largely premised on an assumption that is in no way obviously true: the way the internet *is* benefits individuals. Some of the supposed benefits pointed to are: consumer choice, cheaper costs of doing business, and increased innovation in a wide variety of sectors. However, it has been argued that the one important novelty of the internet is not communication or information; rather, it is the *recording* of human activity. In the analogue world activities can be recorded; however, this very rarely occurs. Online, every tiny movement and interaction is recorded (Ferraris, 2022). This has facilitated the rise of what Shoshannah Zuboff has dubbed 'surveillance

✉ Scott Robbins
sarobbins@protonmail.com

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany

Published online: 16 February 2026

capitalism' (Zuboff, 2019). Surveillance capitalism powers the advertising driven internet and has clearly led to huge profits for large technology corporations – especially during the global COVID-19 pandemic (Jolly, 2021). However, the benefits to consumers are not so clear. Consumers are expected to give up large amounts of sensitive personal information that are used to generate targeted advertisements (Scott, 2020). These targeted advertisements have been associated with election tampering (Crain & Nadler, 2019) as well as a driving force in the dissemination of conspiracy theories leading to genocide (Mozur, 2018), an armed insurrection (Culliford, 2021), and making it much more difficult to get the world vaccinated (Skafle et al., 2022). While I in no way wish to tally up the benefits and negatives of the contemporary internet, it is not clear that the internet, as it is, benefits individual consumers. The fact that attempts at digital sovereignty will cause the internet to fragment – thereby change the way the internet works, does not, therefore, necessarily mean that something bad has happened.

Even if we accept the unproven premise that the internet benefits consumers, there are nonetheless structural issues with the current business model of the internet that must be fixed. The current business model has not been a success and is contributing to the erosion of democracy (as we will see later). A unified, unfragmented internet asks consumers and states to hand over large amounts of sensitive data to other jurisdictions which contribute to this erosion.

The digital advertising market is the lifeblood of the digital economy. Data brokers, for example collect thousands of data points on each internet user in order to generate profiles that are useful to companies and other advertisers. The profiles generated with this data have been used to attack the very foundations of liberal democracy. Furthermore, technology companies have gained an incredible amount of power. Companies use this power to increase profits. They prevent meaningful regulations to keep this power. They have their own benefits – not the benefits of the consumers or society – in mind. These large technology companies are primarily located in two countries: the US and China.[1] An unfragmented internet dominated by, and benefitting, large companies in other countries at the expense of your citizens does not make strategic sense.

Opponents of digital sovereignty may be correct in their analysis that, in the current context, methods to achieve it will cause the internet to fragment. However, too often these opponents seem to defend a status quo that is fundamentally broken and dominated by a few companies which have time and again abused their power.

[1] Although China's dominance may be exaggerated – especially when compared to the United States (Huang & Mayer, 2022).

In this article I will first go over the arguments against digital sovereignty. I will focus on the arguments that digital sovereignty is anti-innovation, protectionist, and authoritarian. On top of that, opponents of digital sovereignty assume that the internet is a success story – that it is good for the state and consumers. However, in I will then show the many ways that the internet has failed us – particularly failed liberal democracy as well as argue against digital sovereignty being anti-innovation, protectionist, and authoritarian. Following this I argue that given this situation, a fragmented internet is the best available option for the state. To be clear, an open, free, unfragmented internet is compatible with liberal democracy. The problem rests not with the internet itself, but with the business model on top of it that has not been properly regulated. It seems, however, that powerful interests are preventing any such regulation from existing – leaving countries who wish to protect their citizens and their democracies with no choice but to 'fragment' the internet.

Digital sovereignty

Digital sovereignty has been used simply to describe "efforts by governments to assert control over online activities" (Chander & Sun, 2022, p. 293). Governments are able to assert control over the seemingly borderless internet because, as Rosenzweig argues, physical location of the servers and data is a practical matter (Rosenzweig, 2012). Therefore, governments are able, through internet service providers located within their jurisdiction, to assert control.

The General Data Protection Regulation (GDPR) in the EU is, perhaps, the first thing that comes to mind when it comes to the exercise of digital sovereignty. It is an attempt to control not only EU companies, but also any company engaging in "processing activities of personal data which have a link to the European Union's territory or market" (Albrecht, 2016, p. 287). This exercise of control over the personal data of EU residents creates constraints for global companies like Alphabet and Meta which have millions of users in the EU. These constraints include limits on the processing of personal data, the transfer of personal data, third-party use of personal data, data retention, and requirements on consent (Hoofnagle et al., 2019).

This article does not take a position on whether the EU's methods (or any other State's methods) are good or bad in terms of establishing digital sovereignty. The arguments against digital sovereignty are arguments against any attempt. I use examples here only to highlight what some jurisdictions are doing. The EU is often used as an example in this debate and this article continues that tradition. Remember that the purpose of this article is to argue that a fragmentation of the internet is not necessarily a bad thing;

on the contrary, given the way the internet functions now, it is the only way forward.

Countries have also attempted to control the location of the personal data of their citizens. These laws are collectively called 'data localization' laws. Australia, for example, has its Personally Controlled Electronic Health Records (PCEHR) act which "prohibits the transfer of health records outside of Australia" (Chander & Le, 2014, p. 6). The Canadian state of British Columbia has a similar law regarding health data (Bannerman, 2024). Russia and China have some of the strictest data localization laws (Yun, 2025; Savelyev, 2016). These are just a couple of examples of the many proposed laws that are attempting in some way to establish digital sovereignty.

Against digital sovereignty

There are several arguments against digital sovereignty. The main thrust of the argument is that the establishment of digital sovereignty will fragment the internet. There will be a US internet, a European Internet, a Russian Internet, a Chinese internet, etc. A unified internet promotes democratic values and users could be cut off from the services that the internet provides (Komaitis, 2023).

The services in question – are on this view – unquestionably good services. They are services we want everyone to have access to. They are services we want to keep on a unified internet. The worry is that, for example, the EU digital services act and GDPR will create a situation in which some services won't be offered in Europe – meaning that the internet in Europe will be different from the internet in the US. This, it is argued, would be bad for Europe and the US.

Furthermore, the establishment of digital sovereignty is claimed by opponents to be anti-innovation, protectionist, and authoritarian.

Anti-Innovation

The organizations and standards that serve as the groundwork for the internet to function are quite numerous and facilitate a large number of easily accessible services. In a matter of minutes, I can put up a website that can be accessed by anyone with an internet connection – which according to the International Telecommunication Union (ITU) is about 4.9 billion people (ITU, 2021). Organizations like ICANN (Internet Corporation for Assigned Names and Numbers) and IETF (Internet Engineering Task Force) then provide the standards and databases which enable, for example, someone to type into their web browser the address to my website. The information that I wish to present, in the way that I want it presented, is shown. All it cost me to do this was around 15 euros to register the domain name for the year and, if I do not have access to server space, another 60 euros per year to host the data for the site.

The top ten companies by market capitalization in the world today include Meta (Facebook), Alphabet (Google), and Amazon. These companies' existence is based on the infrastructure that the internet provides. It is unquestionable that the internet fostered innovation that created many of the services that we now take for granted. The calls for more digital sovereignty can be seen as a threat to the environment of innovation that made these companies what they are.

The General Data Protection Regulation (GDPR) adopted by the EU, for example, may have stalled 40 clinical cancer studies due to confusion about whether these studies would comply with the law (Eiss, 2020). The concern is that GDPR and future laws in a variety of jurisdictions makes it confusing for those trying to conduct clinical research across jurisdictions. It may simply be too costly and difficult to meet the regulatory requirements (Mee et al., 2021).

New legislation in Europe like the Digital Services Act (DSA) has also been seen as anti-innovation. Google has explicitly raised objections to a proposed ban on surveillance advertising in the DSA which, according to them, would hurt consumers and small and medium sized enterprises (SMEs) (Corporate Europe Observatory, 2022). Spotify also raised a concern with a ban on targeted advertising to minors saying "a broad ban on tailored advertising to minors could badly affect the development of free streaming services, which are very popular with young people of different ages" (Corporate Europe Observatory, 2022).

The Center for Strategic and International Studies identified three ways that large companies foster innovation. First, they make it easy for SMEs to immediately gain a large online presence – something that would be impossible to do before. Second, the overall gain in GDP related to these companies (their own business, and the SMEs that they facilitate) makes for greater competition and innovation in a variety of sectors. Third, these companies spend a lot of money on research and development (R&D) which fosters internal innovation (Broadbent, 2020).

Later I argue that laws attempting to establish digital sovereignty are indeed against some forms of innovation; however, only those forms of innovation that rely on practices that have shown to be harmful to citizens or state institutions.

Protectionist

A further argument against digital sovereignty and the supposedly resulting fragmentation of the internet is that, whether intended or not, it is inherently protectionist. Meta has recently claimed that because of European rules it would

"likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe" (Hern, 2023). This could, it is argued, be the intention of digital sovereignty – making it more likely that digital services coming from, in this case, Europe, are to succeed.

Some have compared GDPR to tariffs – which raise the cost of foreign companies to do business. While Meta has not followed through on their threat to withdraw from Europe, many smaller companies offering digital services have simply stopped offering services to European users (Kuchler, 2018). The point that opponents are trying to make is that digital sovereignty and privacy are excuses to promote homegrown companies over foreign ones. Governments "can readily weaponize digital sovereignty to serve protectionist goals" (Chander & Sun, 2022).

Sometimes it is stated that digital sovereignty is protectionist without argument. Mueller (2020), for example, claims that "opportunities for national protectionism would expand exponentially" if digital sovereignty is realized.

Others focus in on data localization laws – claiming that requiring digital service providers to keep data associated with the citizens on servers located within a particular jurisdiction favors large or local companies. Taylor claims that data localization is, "by definition, a form of protectionism" (2020).

I argue in the next section that laws attempting to establish digital sovereignty are not protectionist in that they do not inherently favor companies from any region. They target the practices and services themselves based on how those services are developed and run. Companies from anywhere can decide to follow these laws.

Authoritarian

In the utopian view of the internet, the open and free internet is a threat to authoritarianism. The internet "makes it harder for authoritarian regimes to suppress their citizens" and digital sovereignty will "erode that liberty enhancing feature of the internet" (Chander & Le, 2014, p. 46). The quest for digital sovereignty, it is argued, will support authoritarianism by making it harder for people to gain access to information.

Relatedly, it is argued that digital sovereignty policies will fragment the internet – resulting in an increasing number of smaller and more tightly controlled networks that could be more easily subjected to authoritarian controls and silence unpopular or dissenting information" (Huddleston & Varas, 2020).

Furthermore, policies supporting digital sovereignty can also be used to suppress and surveil citizens. While liberal democracies may not use the policies in this way, these policies set "a precedent for authoritarian governments to reference, which undermines European human rights and foreign policy" (Maurer et al., 2015, p. 15).

I argue later on in the article that authoritarian governments already use the internet to support themselves. And while it is true that authoritarian governments will use the concept of digital sovereignty to oppress their citizens, it does not follow that the concept of digital sovereignty is bad, only that authoritarian governments are bad.

The internet: not a utopia

The first thing that we should notice about the arguments above is that they are arguments for keeping the status quo when it comes to the internet. If we keep the status quo then it is important that the internet is good for states and consumers. The opponents of digital sovereignty operate on a utopic view of the internet that has been thoroughly debunked. While most of the world and the businesses that operate within that world now depend upon the internet – this does not mean that this dependence is good.

Mueller provides an example of the utopic view of the internet had by opponents of digital sovereignty. He says, as if it is obvious, "Suppliers of internet access and services do not "extract" anything from the virtual commons created by mutual use of the internet protocols" (Mueller, 2020, p. 794). What he means by this is that the data is not extracted in the sense that we commonly use the word. For example, when a company extracts fish from the ocean, those fish are gone and no one else can have them. The data recorded by suppliers of the internet haven't taken the data in this way. It is possible for others to record or use the same data. To use his metaphor of the ocean, it would be more like recording the movements and habits of the fish rather than catching them. However, what he fails to point out is that the data is only worth anything when aggregated with the data of millions of other users. The valuable information are the insights that one can glean from this data. Not anyone has the ability to record this data – and therefore are unable to create insights. Only service providers are in a position to record this information. So, while Mueller is correct that internet service providers are not taking things in a way that reduces the availability of that information, the system is setup in such a way that the data is only available to those providers.

The internet 101

The internet is, roughly, a worldwide set of connected computers. Each computer is given an Internet Protocol (IP) address. When you type in a URL address into your browser you send that request first to a Domain Name

Service – which is, to put it simply, a table that lists URL addresses with their corresponding IP addresses. One must register a domain name with a registrar. This is submitted to the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a non-governmental organization which is responsible for assigning IP addresses.

Getting the right address is one part of the problem. The second part is sending and receiving data. This is handled by a protocol called Transmission Control Protocol/Internet Protocol (TCP/IP). This protocol provides a standard set of rules so that computers from all over the world can communicate. Finally, there are many other standard protocols that allow for specialized sending and displaying of information. Common protocols include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP). These protocols allow users to interact with other computers in a standard way – facilitating many of the services that power the internet.

This short description of the internet shows that it only works when the computers on the internet follow the standard protocols. This is great in that individuals and business can reach across the globe to consume and provide services. But it also provides the capability to take advantage of a lack of global guardrails preventing bad actors (in this case including companies) from abusing consumers.

So far, in this article, I have said that I will argue that the best option is for the internet to be fragmented. However, I will not be arguing that the standards which serve as the foundation of the internet listed above should be fragmented. There is nothing about the common standards which facilitate the internet that necessitate it the bad business model which causes the harms below. The internet, as described above, could stay the same.

Surveillance capitalism

The business model of the internet is what Shoshana Zuboff calls "surveillance capitalism." The aim of surveillance capitalism is "to predict and modify human behaviour as a means to produce revenue and market control" (Zuboff, 2019). The ability to predict and modify human behavior is a valuable power. This ability is powered by data. A report by the Federal Trade Commission found that billions of data elements are collected on every individual US consumer. One firm, for example, was found to add 300 billion records (each record is a data element associated with an individual) to its databases each month (in 2014).

Everywhere you go online, and everything you do, is tracked. Each search term you enter, link you click on, video you watch, purchase you make, etc. is collected. This data alone can be used to infer things about you. For example, despite not telling anyone – even your partner – that you are pregnant, the data collected about you could easily give that information away. Internet searches about pregnancy (you might want to ask Google what vitamins you need for a healthy pregnancy) and the fact that you clicked on an article about how to treat nausea during pregnancy might be enough to update your online profile to indicate that you are pregnant. This information is clearly beneficial to advertisers. Pregnant people are likely to be influenced by different types of ads and be more likely to purchase certain products.

This business model, while allowing for many SMEs and large companies to thrive, has sparked an opaque industry of data brokers whose only reason for being is collecting data, combining data, and producing profiles of everyone that is on the internet to then sell to whoever needs it. These data brokers facilitate microtargeted ads which have led to many of major problems that the internet has today.

Data brokers

Data brokers are "companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analyzing, and sharing that information, or information derived from it" (Federal Trade Commission, 2014, p. 3). Uniquely, consumers most often never interact with, or even know about these companies.

These companies collect data from a number of sources and use it to make money in a number of ways. Data brokers collect commercial, governmental, and publicly available data. This information is used to create a "detailed composite of the consumer's life" (Federal Trade Commission, 2014, p. iv). These composites are then used to facilitate services like: people search, targeted advertising, and fraud detection.

It is an understatement to say that data brokers have a lot of data on individual consumers. The US Federal Trade Commission found that one data broker had over 3000 data segments on every US consumer. Data segments are the categories that apply to an individual. This is not only data that they have collected directly, but data that is inferred based on other data. For example, one data broker had data segments like "expectant parent" and "diabetes interest" which gives away health information. One can purchase all the data that these companies have on individuals who, for example, are "Ethnic Second-City Strugglers" referring to low-income people of color (Sherman, 2021).

Once data brokers have all of this data – they sell it as they please. Law enforcement has frequently found a way around laws preventing the collection of location data by purchasing the data from data brokers (Canon, 2020). Immigration and Customs Enforcement (ICE) in the US has evaded laws preventing them from collecting utilities data (data about water and electricity customers) by simply buying the data

from data brokers (Wang et al., 2022). These laws preventing such data sharing were enacted to ensure that the basic human rights of immigrants could be met without fears of being deported.

There is growing concern that the data held by data brokers can be used for malicious purposes and that they may be responsible for what gets done with that data. Epsilon (one of the largest data brokers), for example, had to pay a fine of 150 million USD after being charged for selling data which facilitated elder fraud schemes (US Department of Justice, 2021).

Erosion of democracy

Rather than enhancing democracy, the internet has lately facilitated much to undermine it. In the aftermath of Brexit it was revealed that Russian influence through social media may have been a deciding factor in the UK exiting Europe (Ruy, 2020) is present in the text, but reference is missing in the reference section. Could you please provide the reference or delete the text citation."2020). Furthermore, it has been widely reported the Russian government attempted to influence the 2016 and 2020 US elections – in support of Donald Trump. The U.S. intelligence community released a report detailing the efforts of Russia, Iran, Cuba, Venezuela, and others to use the internet to push certain narratives which would sow division and reduce confidence in the electoral process. The report claims that the Russian government pushed narratives that denigrated Joe Biden and promoted Donald Trump (National Intelligence Council, 2021). The report claims that:

> *The Kremlin -linked influence organization Project Lakhta and its Lakhta Internet Research (LIR) troll farm commonly referred to by its former moniker Internet Research Agency (IRA) amplified controversial domestic issues. LIR used social media personas, news websites, and US persons to deliver tailored content to subsets of the US population (*National Intelligence Council, 2021, p. *4)*.

This is a direct example of using the business model that the internet rests on – surveillance capitalism – to undermine democracy. China used the WeChat messaging service to meddle in Canadian Elections (Peng, 2018) is present in the text, but reference is missing in the reference section. Could you please provide the reference or delete the text citation."2018). China has also used the openness of the internet to collect information on, for example, Indian Citizens (China relied upon Alibaba's cloud servers for this) (Tyagi, 2021). Spreading misinformation by China in the Taiwanese democracy has even led a prominent Taiwanese diplomat to take his own life and cite the spread of this misinformation as a reason (Horton, 2018) is present in the text, but reference is missing in the reference section. Could you please provide the reference or delete the text citation."2018).

These campaigns to undermine democracy work due to the surveillance capitalist infrastructure. The ability to target specific groups for misinformation is extremely powerful. The Vote Leave campaign in the UK was able to have 1433 different advertisements supporting their cause with a wide variety of themes and slogans. Each advertisement was there to push the buttons of certain groups of people "based on their age, where they lived and other personal data taken from social media and other sources" (BBC News, 2018b).

Democracies around the world have to do something to protect themselves from these threats. Those arguing against digital sovereignty are arguing that keeping the internet as a free unified whole is more important than sovereign nations protecting their governmental system.

Against digital sovereignty revisited

Chander and Le provide another example when they say that the free and open internet is "liberty-enhancing" (Chander & Le, 2014). However, the internet is, in fact, facilitating authoritarianism. The arguments that digital sovereignty is anti-innovation imply that the internet fosters innovation. However, the internet is dominated by a few companies (Dolata, 2018) that swallow up many potential competitors (Motta & Peitz, 2021). Furthermore, network effects ensure that their dominance continues without real competition (van der Aalst et al., 2019). The real innovation that the internet has fostered is the ability to create profit from surveilling consumers.

Anti-Innovation?

The innovation most associated with the internet is the provision of services to consumers for no money. Consumers, instead, provide a lot of data which drives advertising. Because this data comes with the harms described earlier, there is a huge cost to this innovation of free services. Democracy itself may be at stake – which is too high a cost. The dependence upon targeted advertising as the business model of the internet drives the erosion of democracy and inherently unethical firms like data brokers. States enacting rules establishing digital sovereignty by limiting these practices (like in the EU) encourage innovating in terms of the business model of the internet. If we want to continue to have the online services we depend on today *and* have a healthy, functioning democracy, then we need the business model of the internet to change (Zuboff, 2019).

It is important to note that many sets of laws attempting to protect something have been charged with being anti-innovation. Environmental protections like the Clean Water and the Clean Air acts, for example, were accused of being anti-innovation (see e.g., Miller, 2023). These laws do stifle innovation that relies upon polluting the air and water; however, these laws encourage innovations that do not pollute (see e.g., Miller, 2023 for discussion)– which is exactly what we want. The problem is that established companies which rely on polluting to make money will be unhappy that they cannot operate as usual. The same situation occurs on the internet. Large technology companies relying upon harmful practices like targeted advertising to make money are unhappy with laws that restrict such practices. However, these laws will encourage new companies to innovate in ways that do not rely upon such practices.

Innovation cannot simply be used as a buzzword for something good. Innovation is often bad. The innovation in the US of 'bump stocks' which turn semi-automatic rifles into fully automatic rifles (circumventing a law outlawing fully automatic rifles) is an innovation, for example, that we do not want. Laws will always restrict some form of innovation – but promote other forms at the same time. The establishment of digital sovereignty is against some forms of innovation – those forms relying on a business model or practices that are harmful to the state's citizens or institutions.

Even within the current internet, innovation has a problem. It is mostly large companies that benefit. It is difficult to start a new social media service that directly competes with another. Individuals may think the new service is better; however, social media requires a large number of users to make the service useful. This is the network effect – which says that the more people in one's circle using a particular service makes it more likely that the person in question will use that service as well. This is another way to say that the choice of using a particular online service is often based on whether others are using it. This gives the established services an advantage as changing services requires whole groups to change. This problem was recently experienced by many who wanted to use Mastadon instead of Twitter after the purchase of Twitter by Elon Musk. Although Mastadon could be a better, more ethical, service – its usefulness is dependent upon the others in your network using it as well.

Furthermore, the data that is held by established large technology companies allows them to prevent start-ups from becoming real challengers. Investors have described so-called 'kill-zones' where certain categories of start-ups receive no investment because large technology companies have made their intention to kill possible competitors in this area. This discourages innovation in these areas as it will be hard to get funded (Regard, 2021).

This is why the DSA and other legislation in Europe has been proposed explicitly to foster innovation. The European Commission's website explicitly states that with the DSA "unnecessary legal burdens due to different laws will be lifted, fostering a better environment for innovation, growth and competitiveness, and facilitating the scaling up of smaller platforms, SMEs and start-ups" (European Commission, 2022a). This is often framed in terms of large online gatekeepers like Facebook, Amazon, and Google preventing SMEs from thriving because of network effects and anti-competitive practices. The DSA, for example, has proposed that large online gatekeepers share their data with SMEs in order to make it easier for them to enter the market.

The internet has fostered innovation such that many of the services, we now take for granted would not exist without it. However, these same services could exist without the targeted advertising business model that exists today. ProtonMail, for example, provides virtually the same service as Gmail. The difference is that this service is provided without advertising as the business model. Privacy and security are the driving values of ProtonMail. ProtonMail makes money by charging consumers directly for the service. Services like ProtonMail may be a glimpse of an ethical future for the internet – one in which services are provided without relying upon the harmful data-driven advertising practices happening today.

To be clear, services like ProtonMail would not come about simply because the internet was fragmented. The point is that if geographic regions were able to setup rules to protect their citizens which prevent some of the business practices used by major internet service providers today, then these constraints would give opportunities for innovation in how internet services are provided that are in accordance with the values of the geographic region exercising its sovereignty (Acar et al., 2019).

Protectionist?

The accusation that digital sovereignty is protectionist rests on a flimsy argument. The idea is that enacting laws which increase digital sovereignty for a particular state effectively privileges the companies that reside in that state. Europe's GDPR, Digital Services Act and, AI act, then, privilege companies operating within the EU because existing companies residing primarily elsewhere will have their business model's hurt by such policies. Some have even made the analogy to tariffs.

However, unlike tariffs, there is nothing inherent to these policies that privilege a company based on its location. These policies privilege companies based on the functioning of its services. Even those arguing against digital sovereignty have admitted that "GDPR compliance differs

from Trump's protectionism in one important respect: that domestic European firms must incur the same costs as American firms" (Lyons, 2018).

Because large American companies dominate the digital services market, it is of course true that they are more affected than upstart European companies that can build GDPR compliance into their services from the start. However, the argument for privacy laws like GDPR is that certain practices are violating the privacy of consumers – which is enshrined in the Universal Declaration of Human Rights.

The EU recently moved to ban products which are made using forced labor (European Commission, 2022b). This ban will affect many industries as it is estimated that over 27 million people are in forced labor around the world. It does not seem to matter if forced labor only occurred outside of Europe or in one particular country. The ban would have the effect of costing those companies relying on forced labor a lot of money – and privileging those companies that do not use forced labor – which may be many European companies. But this is exactly what we want – to privilege companies that don't violate human rights over ones that do violate human rights. Those arguing that privacy laws and the establishment of digital sovereignty incurs significant costs on American companies are simply admitting that those companies are violating human rights.

In sum, many laws seeking to establish digital sovereignty are not protectionist. They protect against companies engaging in harmful practices – which has been done throughout history to protect human rights, the environment, and consumers health. There is nothing stopping companies from any part of the world offering services that do not engage in these harmful practices. Therefore, these digital sovereignty laws cannot be described as protectionist.

Already authoritarian

The accusation that digital fragmentation is authoritarian has some intuitive plausibility. Whenever we think of the internet being fragmented the first example that comes to mind is the great firewall of China. China has indeed used the internet to realize authoritarian ends. They have stifled free speech by imposing harsh prison terms on internet users who express dissent online and restricted what information can be shown online (by forcing companies to filter their results) (Shahbaz & Funk, 2021).

However, the free and open internet is also subject to authoritarianism due in part to authoritarian regimes using the internet to further their political objectives elsewhere – including liberal democracies (see e.g., Mahoney, 2022; Mayer, 2020). It is estimated that over 70 states have cross-border political disinformation campaigns relying upon social media (Blackwood, 2020). The fact that anyone can post information to social media, targeted advertising, and provocative information spreading faster than information trying to counteract it, makes the internet a powerful tool to support authoritarian regimes (Blackwood, 2020). Authoritarian actors like China and Russia also use this technique of 'flooding' to cause political instability in their rivals. This is the technique of creating many posts with a preferred message in order to drown out undesirable information.

Anti-democratic movements within liberal democracies also use social media to spread misinformation and gain attention using these same techniques. The populist movements of Trump in the US, National Rally in France, PVV in the Netherlands, Pegida and AFD in Germany, etc. have all amplified their profiles using online tools (Tucker et al., 2017).

Furthermore, the argument that digital sovereignty can be wielded by abusive governments for authoritarian control is weak. Legal systems and laws can be wielded by abusive governments. A military and the police can be wielded by abusive governments for control. That is NOT an argument against these things – only an argument that abusive governments are bad.

To claim that digital sovereignty is inherently authoritarian would require much more evidence than authoritarians using the concept to suppress their citizens. Opponents of digital sovereignty would need to show that the methods to obtain digital sovereignty cause authoritarianism. So far it has only been shown that authoritarians also use digital sovereignty. Even if this was proved, however, it would also have to be shown that digital sovereignty is more of a cause of authoritarianism than the internet as it stands.

Broken promises

With the internet we were promised that we would be more informed, more connected, and freer. Unfortunately, these promises have been broken. While access to information is better than ever, the rise of social media has led to a surge in misinformation that undermines everything from fair elections to the ability of the state to control a pandemic (Bennett & Livingston, 2018). While there is more communication than ever due to the internet, there are now serious concerns that it is causing a mental health crisis amongst teens (Hilal Bashir & Shabir Ahmad Bhat, 2017) is present in the text, but reference is missing in the reference section. Could you please provide the reference or delete the text citation."2017) and that this online form of communication actually leaves us less connected than ever – what Sherry Turkle calls being "Alone, Together" (Turkle, 2011).

Moreover, societies do not reap the benefits of tax revenue due to the high profitability of large internet companies. The EU commission claims that the biggest companies

pay an average tax rate of 9.5%. Traditional companies pay 23.3% (BBC News, 2018a). Large technology companies do everything they can to pay less taxes (Neate & correspondent, 2021). As tech companies replace traditional companies, this has serious effects on the state's ability to fund its services.

Accepting a fragmented internet

It is intuitively reasonable and desirable to have a unified internet. One where information can travel unobstructed across borders. In a perfect world, where there are non-malicious actors, and global companies can be trusted, we should indeed do everything we can to keep a unified internet. However, the world is not perfect. Companies have used the internet to extract as much personal information as possible from consumers – without meaningful consent. This information is used for purposes that end up hurting consumers as well as the state.

With non-digital goods states have rules about what is allowed in, and what specifications those products must have. Everything from car seats for babies to food products have requirements that must be met in order to be imported into the state. This is to prevent harm to the state and its citizens. It is unreasonable to expect digital products and services, given the harm that we now know can be caused, to be treated differently.

Critics of digital sovereignty argue that there are massive benefits to keeping a unified internet. However, those benefits are not evenly distributed. The United States derives many of these benefits while all states and their citizens are hit by the harm. Even in the US, however, large technology companies have stifled innovation and competition by simply buying any start-up that begins to do well. Critics also argue that digital sovereignty is simply a ruse to enact protectionist measures – favoring their own companies. However, policies to establish digital sovereignty simply create rules over the digital that any firm can follow. When the EU establishes safety rules for baby seats, they do not favor EU companies. They are protecting EU citizens from potential harm caused by unsafe baby seats. Any firm can decide to follow those rules.

A better way to protect consumers and states from the potential harm that comes from the internet may be to establish global rules – keeping a unified internet. However, until these rules are strong enough to protect the consumers in question – states will have to establish their own rules. Companies are simultaneously calling for global regulation to prevent digital sovereignty as well as spending millions to prevent meaningful global regulation from being established (Edgerton & Birnbaum, 2022; Goujard, 2022).

Not establishing rules that protect citizens from a toxic business model and abuses by large technology companies is ceding state power to large technology companies who have a conflict of interest when it comes to the care of consumers. Fixing the problems highlighted in this paper would require a different business model. However, there is no incentive for big technology companies to change.

Rules establishing sovereignty over the digital may indeed create different zones within the internet. Europeans may not have access to some services offered by US companies. Some services will be different in different regions. The cost of offering a specific service in a certain region may simply be too high due to regional regulations. But states have a duty first and foremost to their citizens and the well-functioning of society. It is now clear that these services put the privacy of citizens and the functioning of the democratic state at risk.

The fragmentation of the internet is an expression that brings to mind a world in which people live behind something like the great firewall of China. They don't have access to information that they should have access to. This is not the case though. Europe, for example, is not dictating what information is allowed to be accessed in Europe – only that certain surveillance and advertising methods are banned (e.g., sharing personal data without consent). Fragmentation, rather than be seen as a dystopia, can be seen as the state creating an oasis where consumers are safe from harmful practices that underly many digital services.

To be clear, fragmentation is not desirable in and of itself. A state should not be seeking to fragment the internet. Fragmentation is a choice that companies make in response to digital legislation. When they say it is too difficult to provide their services given new laws, they are threatening fragmentation of the internet unless states refrain from protecting their citizens. A fragmented internet, therefore, is something states are forced to accept if they want to protect their citizens.

Acknowledgements Thanks to Maximilian Meyer and Inga Blundell for helpful discussions and comments on earlier drafts.

Author contributions S.R. wrote the main manuscript text as well as reviewed and edited it.

Funding Open Access funding enabled and organized by Projekt DEAL.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

Acar, O. A., Tarakci, M., & van Knippenberg, D. (2019). Creativity and innovation under constraints: A Cross-Disciplinary integrative review. *Journal of Management*, *45*(1), 96–121. https://doi.org/10.1177/0149206318805832

Accenture. (2017). *Digital fragmentation' poses threat to businesses' global growth and innovation according to accenture report*. Accenture. https://news/digital-fragmentation-poses-threat-to-businesses-global-growth-and-innovation-according-to-accenture-report.htm

Albrecht, J. P. (2016). How the GDPR will change the world forword. *European Data Protection Law Review (EDPL)*, *2*(3), 287–289. https://heinonline.org/HOL/P%26h=hein.journals/edpl2%26i=313

Bannerman, S. (2024). Platform imperialism, communications law and relational sovereignty. *New Media & Society*, *26*(4), 1816–1833. https://doi.org/10.1177/14614448221077284

BBC News (2018a, March 21). Technology giants face European digital tax blow. *BBC News*. https://www.bbc.com/news/business-43486403

BBC News (2018b, July 26). Vote leave's targeted brexit Ads released by Facebook. *BBC News*. https://www.bbc.com/news/uk-politics-44966969

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of Democratic institutions. *European Journal of Communication*, *33*(2), 122–139. https://doi.org/10.1177/0267323118760317

Blackwood, K. (2020). *Kreps: Social media helping to undermine democracy*. *Cornell Chronicle*. https://news.cornell.edu/stories/2020/08/kreps-social-media-helping-undermine-democracy

Broadbent, M. (2020). *The Digital Services Act, the Digital Markets Act, and the New Competition Tool*. Center for Strategic and International Studies. https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool

Canon, G. (2020, December 3). ACLU files request over data US collected via Muslim app used by millions. *The Guardian*. https://www.theguardian.com/us-news/2020/dec/03/aclu-seeks-release-records-data-us-collected-via-muslim-app-used-millions

Chander, A., & Le, U. P. (2014). *Breaking the Web: Data Localization vs. the Global Internet* (SSRN Scholarly Paper ID 2407858). Social Science Research Network. https://papers.ssrn.com/abstract=2407858

Chander, A., & Sun, H. (2022). Sovereignty 2.0. *Vanderbilt Journal of Transnational Law*, *55*(2), 283–324. https://heinonline.org/HOL/P%26h=hein.journals/vantl55%26i=299

Cohen, B., Hall, B., & Wood, C. (2017). Data Localization Laws And Their Impact on Privacy, Data Security And the Global Economy. *Antitrust*, 32(1), 15. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/antitruma32&section=22&casa_token=i86fesaPKj0AAAAA:tXqUAbhgrqjnu3ucQaG1RVYDKHCUeMmT0YQE-8Gktc71e4qLHlDDl1Qu5i9Mrsw7yfLKvG0T-w

Corporate Europe Observatory (2022, April 23). *Big Tech's last minute attempt to tame EU tech rules | Corporate Europe Observatory*. https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules

Crain, M., & Nadler, A. (2019). Political manipulation and internet advertising infrastructure. *Journal of Information Policy*, *9*, 370–410. https://doi.org/10.5325/jinfopoli.9.2019.0370

Culliford, E. (2021, January 12). Online misinformation that led to Capitol siege is radicalization, say researchers. *Reuters*. https://www.reuters.com/article/us-misinformation-socialmedia-idUSKBN29H2HM

Dolata, U. (2018). Internet Companies: Market Concentration, Competition and Power. In U. Dolata & J.-F. Schrape (Eds.), *Collectivity and Power on the Internet: A Sociological Perspective* (pp. 85–108). Springer International Publishing. https://doi.org/10.1007/978-3-319-78414-4_5

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. World Economic Forum. https://doi.org/10.5167/uzh-121102

Edgerton, A., & Birnbaum, E. (2022, September 6). Big Tech's $95 Million Spending Spree Leaves Antitrust Bill on Brink of Defeat. *Bloomberg.Com*. https://www.bloomberg.com/news/articles/2022-09-06/tech-giants-spree-leaves-antitrust-bill-on-brink-of-defeat

Eiss, R. (2020). Confusion over europe's data-protection law is stalling scientific progress. *Nature*, *584*(7822), 498–498. https://doi.org/10.1038/d41586-020-02454-7

European Commission (2022a, May 20). *Questions and Answers: Digital Services Act* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

European Commission (2022b, September 14). *Commission moves to ban products made by forced labour* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5415

EY Consulting. (n.d.). *The fragmentation of everything*. MIT Technology Review. Retrieved June 2 (2021). from https://www.technologyreview.com/2020/12/04/1013038/the-fragmentation-of-everything/

Federal Trade Commission, U (2014). *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014)*. Federal Trade Commission. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

Ferraris, M. (2022). Webfare: Humanity's greatest asset. *Journal of E-Learning and Knowledge Society*, *18*(3), 29–35. https://doi.org/10.20368/1971-8829/1135817

Floridi, L. (2020). The fight for digital sovereignty: What it Is, and why it Matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Goujard, C. (2022, October 14). Big Tech accused of shady lobbying in EU Parliament. *POLITICO*. https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban/

Hern, A. (2023, May 23). TechScape: Warnings of a 'splinternet' were greatly exaggerated – until now. *The Guardian*. https://www.theguardian.com/technology/2023/may/23/techscape-splinternet-meta-facebook-fine

Hilal Bashir & Shabir Ahmad Bhat. (2017). Effects of social media on mental health: A review. *International Journal of Indian Psychology*, *4*(3). https://doi.org/10.25215/0403.134

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Horton, C. (2018, November 22). *Specter of Meddling by Beijing Looms Over Taiwan's Elections—The New York Times*. https://www.nytimes.com/2018/11/22/world/asia/taiwan-elections-meddling.html

Huang, Y., & Mayer, M. (2022). Power in the age of datafication: Exploring china's global data power. *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-022-09816-0

Huddleston, J., & Varas, J. (2020, June 16). *Impact of Data Localization Requirements on Commerce and Innovation*. American Action Forum. https://www.americanactionforum.org/insight/impact-of-data-localization-requirements-on-commerce-and-innovation/

ITU (2021). *Measuring digital development: Facts and figures*. *International Telecommunications Union*. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Jolly, J. (2021, May 1). *'It's just the beginning': Covid push to digital boosts big tech profits*. The Guardian. http://www.theguardian.com/business/2021/may/01/its-just-the-beginning-covid-push-to-digital-boosts-big-tech-profits

Komaitis, K. (2023). *Internet Fragmentation: Why It Matters for Europe*. EU Institute for Security Studies. https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/ioyLip9O/internet-fragmentation-why-it-matters-for-europe.pdf

Kuchler, H. (2018, May 24). US small businesses drop EU customers over new data rule. *Financial Times*. https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04

Lyons, D. (2018, July 3). GDPR: Privacy as Europe's Tariff by Other Means? *American Enterprise Institute - AEI*. https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/

Mahoney, J. G. (2022). China's rise as an advanced technological society and the rise of digital orientalism. *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-022-09817-z

Maurer, T., Skierka, I., Morgus, R., & Hohmann, M. (2015). Technological sovereignty: Missing the point? *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, *53-68*. https://doi.org/10.1109/CYCON.2015.7158468

Mayer, M. (2020). China's Authoritarian Internet and Digital Orientalism. In D. Feldner (Ed.), *Redesigning Organizations: Concepts for the Connected Society* (pp. 177–192). Springer International Publishing. https://doi.org/10.1007/978-3-030-27957-8_13

Mee, B., Kirwan, M., Clarke, N., Tanaka, A., Manaloto, L., Halpin, E., Gibbons, U., Cullen, A., McGarrigle, S., Connolly, E. M., Bennett, K., Gaffney, E., Flanagan, C., Tier, L., Flavin, R., & McElvaney, N. G. (2021). What GDPR and the health research regulations (HRRs) mean for ireland: A research perspective. *Irish Journal of Medical Science*, *190*(2), 505–514. https://doi.org/10.1007/s11845-020-02330-3

Miller, A. S. (2023). Environmental Regulation, technological Innovation, and Technology-Forcing. *Natural Resources & Environment*, *10*(2), 26–69. https://www.jstor.org/stable/40923453

Motta, M., & Peitz, M. (2021). Big tech mergers. *Information Economics and Policy*, *54*, 100868. https://doi.org/10.1016/j.infoecopol.2020.100868

Mozur, P. (2018, October 15). A Genocide Incited on Facebook, With Posts From Myanmar's Military. *The New York Times*. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mueller, M. (2022). *Digital sovereignty: What does it mean?>* Georgia Tech Internet Governance Project. Retrieved April 12, 2024 from https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf

National Intelligence Council (2021). *Foriegn Threats to the 2020 US Federal Elections* (ICA2020-00078D). National Intelligence Council. https://int.nyt.com/data/documenttools/2021-intelligence-community-election-interference-assessment/abd0346ebdd93e1e/full.pdf

Neate, R. (2021, May 31). & correspondent, R. N. W. 'Silicon Six' tech giants accused of inflating tax payments by almost $100bn. *The Guardian*. https://www.theguardian.com/business/2021/may/31/silicon-six-tech-giants-accused-of-inflating-tax-payments-by-almost-100bn

Peng, J. (2018, October 16). Vancouver society at centre of vote-buying allegations has ties to Chinese government. *The Toronto Star*. https://www.thestar.com/vancouver/2018/10/16/vancouver-society-at-centre-of-vote-buying-allegations-has-ties-to-chinese-government.html

Regard, M. (2021). *Venture Capital Kill Zones: Defining Harm to Consumers by Big Tech's Long Shadow*. Vanderbilt University. https://www.vanderbilt.edu/jetlaw/2021/03/13/02/

Rosenzweig, P. (2012). International governance framework for Cybersecurity, the. *Canada-United States Law Journal*, *37*(2), 405. https://scholarlycommons.law.case.edu/cuslj/vol37/iss2/10

Ruy, D. (2020, July 21). *Did Russia Influence Brexit?* https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

Savelyev, A. (2016). Russia's new personal data localization regulations: A step forward or a self-imposed sanction? *Computer Law & Security Review*, *32*(1), 128–145. https://doi.org/10.1016/j.clsr.2015.12.003

Scott, M. (2020, October 23). *Europe is going after the internet's business model. A new one is urgently needed*. POLITICO. https://www.politico.eu/article/online-advertising-privacy-europe/

Shahbaz, A., & Funk, A. (2021). *FREEDOM ON THE NET 2021: The Global Drive to Control Big Tech*. Freedom House. https://freedomhouse.org/sites/default/files/2021-09/FOTN_2021_Complete_Booklet_09162021_FINAL_UPDATED.pdf

Sherman, J. (2021, April 13). Data Brokers Are a Threat to Democracy. *Wired*. https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/

Skafle, I., Nordahl-Hansen, A., Quintana, D. S., Wynn, R., & Gabarron, E. (2022). Misinformation about COVID-19 vaccines on social media: Rapid review. *Journal of Medical Internet Research*, *24*(8), e37367. https://doi.org/10.2196/37367

Taylor, R. D. (2020). Data localization: The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From liberation to turmoil: Social media and democracy. *Journal of Democracy*, *28*(4), 46–59. https://doi.org/10.1353/jod.2017.0064

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

Tyagi, G. (2021, June 12). *Battling Chinese Big Tech encroachment in India*. Observer Research Foundation. https://www.orfonline.org/expert-speak/battling-chinese-big-tech-encroachment-in-india/

US Department of Justice (2021, January 27). *Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes*. The United States Department of Justice. https://www.justice.gov/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes

van der Aalst, W., Hinz, O., & Weinhardt, C. (2019). Big digital platforms. *Business & Information Systems Engineering*, *61*(6), 645–648. https://doi.org/10.1007/s12599-019-00618-y

Wang, N., McDonald, A., Bateyko, D., & Tucker, E. (2022). *American Dragnet: Data-Driven Deportation in the 21st Century*. Center on Privacy and Technology at Georgetown Law. https://americandragnet.org/.

Yun, H. (2025). China's data sovereignty and security: Implications for global digital borders and governance. *Chinese Political Science Review*, *10*(2), 178–203. https://doi.org/10.1007/s41111-024-00269-9

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (1 edition). PublicAffairs.