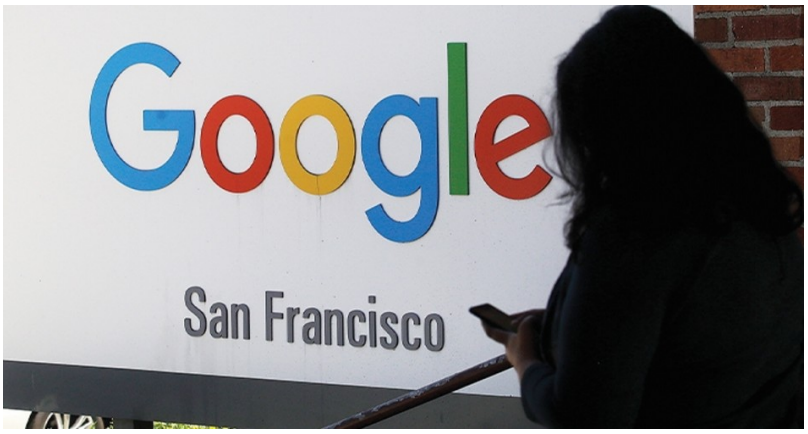
New American

Written by **C. Mitchell Shaw** on January 20, 2020

Published in the January 20, 2020 issue of the New American magazine. Vol. 36, No. 02

Freeing the Web From Big Tech



AP Images
AP Images

Last summer, Facebook slapped this magazine's parent organization, The John Birch Society, with a "hate speech" violation and demonetized the organization's Facebook page for 30 days. The reason: Our July 8, 2019 print magazine cover, which included a real photograph of immigrants illegally crossing a border fence. That cover article was headlined "Immigrant Invasion" and a caption for that photo inside the magazine included the word "diseases." Disregarding the accuracy of the photo, the headline, and the caption, Facebook deemed the post "hate speech."

As a result of the public backlash following this magazine publishing an article about that "hate speech" violation, Facebook backed down. But the fact remains that such actions by Facebook and other social-media giants are not "isolated incidents" — they are par for the course. And while this magazine had the clout to bring pressure to bear on Facebook, individual users who find their posts removed for non-existent violations don't have that clout. They just have to deal with it.

It is a fact beyond honest dispute that "Big Tech" is nearly — if not completely — synonymous with "liberal." The evidence of the past few years has clearly demonstrated that liberals have used Big Tech as a tool to push the world closer and closer to their vision for it — a world where liberalism is the only view, all others having been demolished. Both the Internet and the Web have been used as pivotal tools in that leftward push. As the Web continues to evolve technologically, there is both the danger that the trend toward liberal totalitarianism will continue, and the hope that the stranglehold which makes that trend possible will be broken.

Big Tech has held both the Internet and the Web in a stranglehold for more than a decade. And it has only gotten worse over that time. Censorship, shadow banning, data mining, data manipulation, and user manipulation are the norm.

The Web began in freedom: freedom of speech, freedom of intellectual diversity, freedom of information, freedom of expression. As the Web grew up out of the Internet, it was a digital public square where ideas were disseminated freely and debated openly and honestly. Dissenting opinions were encouraged, not silenced or deleted.

The early Web (known as Web 1.0) was also free from surveillance. In the decades since its creation, the Web has undergone a shift at the hands of Big Tech. The current iteration is increasingly less free and has been designed for the collection of users' data. Thanks to recent developments, that may soon be changing for the better — and we may see a return to the free and unsurveilled Web of the past.

Written by **C. Mitchell Shaw** on January 20, 2020

Published in the January 20, 2020 issue of the New American magazine. Vol. 36, No. 02

The Problem: The Web Is Broken

As Web 1.0 gave way to Web 2.0 (the current iteration), the promise was one of greater user interaction. Sadly, with the advent of social media and other platforms, that promise was not universally kept. Increasingly, it has become apparent that liberal points of view are given preference over conservative points of view. In fact, conservative viewpoints are often deemed "hate speech" or as some violation of a code of conduct and are deleted, as the above account of what happened to this magazine illustrates.

As the *Wall Street Journal* reported in an October 26 article entitled "Tech Giants Have Hijacked the Web. It's Time for a Reboot," there is a growing movement to steal the Web back from the tech giants that have hijacked it for their own purposes. To understand this, it is helpful to understand how the Web was hijacked to begin with.

The shift from a Web of freedom to a monopolistic Web of both censorship and surveillance was made possible because of centralized control of the Web.

First, it should be understood that the Internet and the Web, though often discussed as if they are the same thing, are actually two separate — but related — entities. The Internet (literally an "internetwork" or a network made up of smaller networks) is the infrastructure that makes connections between computers all over the world possible. The Web (World Wide Web, abbreviated www) is the collection of websites that use the infrastructure of the Internet. Think of the Internet as the hardware and the Web as the software.

While it is true that no one company or service has full control of either the Internet or the Web, it is also true that a handful of Big Tech companies and services maintain a disproportionate control of the way people access them and interact on them. Far from the origins of the Internet and Web as places where freedom was the norm, the experience of the average user today is one of restriction. That shift is the result of most Web companies' move to control the flow of as much data as possible.

That control takes two major forms. First (and perhaps most obvious) is — as has been the case with companies such as Facebook, Twitter, and Google — the propensity of social-media sites and other platforms to block access to certain information (or at least make it difficult to find) while promoting other information. Evidence of this was rife during the 2016 election, when Google, Facebook, and others were found to be manipulating search results, users' timelines, and other data points to benefit Hillary Clinton and hurt Donald Trump. That manipulation has only continued and worsened since Trump's electoral victory upset, as can be seen in the way his presidency and the impeachment inquiry against him have been portrayed on platforms controlled by Big Tech. Conservative posts languish in shadow ban prison, while liberal posts enjoy widespread distribution. It can also be seen in Google searches, which quickly return the liberal-approved results, instead of what is either most relevant or most popular.

The second form of controlling data is one of distilling user data down to its most powerful form and then using that data against those users. This is at least as nefarious as the first form, since data mining and data analysis can be used in ways that data manipulation cannot. By collecting vast amounts of personal data from various points, Big Tech is able to funnel users' data into startlingly accurate dossiers on each user. Since both the mining and analysis are done by computer algorithms instead of

by humans, the end result is not a matter of guesswork, but of cold, hard facts. Using that information, Big Tech could easily have even greater control of those users in the future. Data is power and can be used to manipulate users in ways of which those users are unaware. Facebook, for instance, has been found to have used data collected from users to conduct psychological experiments on those users to affect their moods and decisions.

The Solution: Decentralize the Web

The imbalance of power in the digital space — heavily weighted in favor of a few Big Tech companies at the cost of the privacy and liberty of nearly all users — is unacceptable to those who recognize the need for a free and unhindered Web where censorship and surveillance are not the norm. Perhaps first among those who envision — and are working toward — that free and unhindered Web is Sir Timothy Berners-Lee, who is widely known as the "Godfather of the Web." And for good reason: Besides his other many and varied accomplishments, he invented the Web 30 years ago.

In fact, Berners-Lee is fighting the battle for online privacy and liberty in at least two important ways. Besides leading the nonprofit World Wide Web Foundation, which has launched a "Contract for the Web" initiative to put forth a Bill of Rights for the Web to clearly define users' rights, he has also privately helped launch a company called Inrupt, which is developing a protocol called Solid. That protocol would allow users to protect their personal online data by placing those data in a secure container (called a POD) that users can access by verifying their identities.

Users could then share whatever they wanted, but rather than it being stored on the server of the website or platform, such as Facebook, it would display on that site but remain in the POD where the user maintains control of it. Since the companies that operate websites would not host that data, they could not control it. The basic idea is one of digital rights mirroring rights in the real world. Since it is your data, it belongs to you, and should have the same protections as all of your other property.

Since control of users' data amounts to control of users, Berners-Lee and his Inrupt co-founder, John Bruce, recognize that the solution is to return that control to the users themselves. The homepage of Inrupt explains, "When Sir Tim Berners-Lee invented the web, it was intended for everyone. The excitement and creativity of its early days were driven from the notion that we can all participate — and the impact was world-changing. But the web has shifted from its original promise — and it's time to make a change. We can still unlock the true promise of the web by decentralizing the power that's currently centralized in the hands of a few. How? By using the power of Solid. Solid is the technically potent open-source platform built to decentralize the Web. Inrupt is the company that's helping to fuel Solid's success."

Inrupt is not the only emerging power in the privacy struggle. David Chaum, a computer scientist who built the first working digital currency in the 1990s and today is building a new Internet platform called Elixxir, told the *Journal*, "You don't have to control things to exert power in the information space. Just knowing a lot about everybody lets you manipulate the whole situation."

Since both the Internet and the Web have become centralized by a few powerful companies, Chaum's Elixxir aims to decentralize the Web by creating a new model for the Internet. The model: linking users' computers together to share data and — in some cases — processing power by allowing them to "work together by a decentralized randomized algorithm" using encrypted connections for "increased privacy

and network integrity," according to the platform's website.

As the *Journal* article explains, "Websites and apps might look the same — and still be connected to the internet that we know — but companies wouldn't be able to amass data, and they might not even need to build massive cloud-server centers just to run their sites." By keeping personal data in secure locations and only sharing access when and where they choose, users would be able to exercise the most fundamental property of data ownership.

The revolution to shape Web 3.0 has begun, and there appears to be a good chance that while it will be built on newer, better, and more powerful tech than Web 2.0, it may well have the privacy-oriented and freedom-oriented values of Web 1.0 — especially if platforms such as Inrupt's Solid, Chaum's Elixxir, and other emerging tech help shape it and empower users to reclaim their data rights.

The real value of Solid, Elixxir, and others, which we will cover later in this article, cannot be understood without understanding the value of protocols. Protocols are standards that developers use when writing the code for their applications. A good example is HTTP — the basic protocol for the Web. Because it is a standard to which everyone agrees, developers are able to create web browsers that are able to display web pages. That is why it doesn't matter whether you use Firefox, Chrome, Safari, Brave, or some other browser: Web pages all display almost exactly the same on all browsers.

As a result of the nature of the Solid protocol, applications written using it would all allow users to maintain control of their data even while posting pictures and other content to social-media sites, so long as those sites adhered to the protocol. Working alongside existing protocols such as HTTP, Solid, Elixxir, and other privacy-friendly protocols would go a long way toward a Web 3.0 that values the God-given rights of users.

Digital Jails

But as Todd Weaver of Purism told *The New American*, many of the services and platforms on the Web — particularly those offered by Big Tech — do not currently employ protocols that respect privacy or the data-ownership rights of users. While there are open source protocols that value freedom and privacy, companies such as Facebook and Google deliberately ignore those protocols and create their own protocols that limit users' choices, liberty, and privacy. Or worse, they use some elements of those protocols, but deliberately break them to create what Weaver calls "digital jails."

It remains to be seen whether Facebook, Google (which owns YouTube), and other Big Tech companies will adopt protocols such as Elixxir and Solid, but given the weight Berners-Lee carries, it is likely they will feel the need to do so. If not, a decentralized Web still would foster the type of competition that would free both the Web and its users from the tyranny of the current monopoly.

Weaver, whose background is in hardware manufacturing and software development, explained "digital jails" by pointing out that a Facebook Messenger user cannot message an Instagram user, even though both are messaging services and Facebook now owns Instagram. That is because Instagram was originally written to its own proprietary protocol. Ditto Facebook Messenger. Tech companies — especially Big Tech and those seeking to join their ranks — do that to limit interoperability and grow their platforms by force. Once a user begins using one platform, he is "locked in" by being unable to communicate with other users of that platform if he leaves that platform.

Weaver explained that if user A signs up for Facebook Messenger and user B signs up for Instagram,

the only way for them to chat with each other is for one of them to convince the other to adopt the other's platform of choice.

"Can you imagine if you bought a phone from Verizon and your friend bought their phone from AT&T and you couldn't call each other?" Weaver asked. "The reason you can call from one carrier to another is because there is a protocol that handles that."

Weaver explains that it has to be understood that Facebook, Google, and other Big Tech companies are obligated to do what they do. "They have a legal responsibility to their stock holders to put profits first." This fiduciary responsibility seems to serve as a convenient excuse for the data mining, data manipulation, and censorship that are the standard operating procedures for Big Tech. It seems as though the powers-that-be at Facebook, Google, and other Big Tech companies believe the only way to make a profit is to control people and steal their data. Weaver's Purism is proving that profitable capitalism is not at odds with respecting the rights of users.

As a "Social Purpose Corporation" (SPC), Purism is obligated — first and foremost — to its "Social Purpose," which is to foster privacy and the data rights of individuals. Everyone who invests in Purism is made to understand that while profits do matter, they take a back seat to privacy. Weaver told *The New American* that this means that not only does Purism not have to be evil and do the things Big Tech does to make a profit, but because of the company's SPC status, they are legally obligated not to be evil. This does not mean that Weaver thinks making a profit is evil — Purism will always seek to make a profit, only without violating its social purpose.

Digital Rights: You Own Your Data

Purism has been making a name for itself for years now, manufacturing laptops that are built on open source hardware and software. Their laptops are the most secure, privacy-oriented laptops available. Period. Not only is every chip, circuit, and line of code designed for privacy, the laptops have hardware kill switches for the WiFi/Bluetooth and cameras/microphones.

Weaver told *The New American* that the laptops were not his original — or ultimate — goal. He had always intended to build a privacy-friendly phone. The laptop end of Purism was both a "proof-of-concept" and a way to establish both a supply chain and a customer base. That goal now accomplished, Purism has released an early version of the Librem 5, a Linux-powered smartphone that goes even further toward respecting and protecting users' privacy.

The impetus for the creation of the Librem 5 phone was the birth of Weaver's daughters. He told *The New American* that after the birth of his second daughter, he realized he was raising two young girls in a world where corporate and government surveillance are the norm. That was unacceptable to him. He knew how to lock an Android phone down and limit most of the surveillance, but told *The New American*, "It's not easily duplicatable."

This writer can sympathize with Weaver's dilemma, having for years now used an Android phone that I modified to remove all things Google. By running an aftermarket operating system that spoofs Google Play Services, I am able to install and run apps that require it. By using privacy-respecting apps such as Signal — which requires Google Play Services to notify me of incoming text messages — and ProtonMail, I have greatly re-established the trustworthiness of my phone. But it is an ongoing project to keep everything up-to-date. It is not something I can do for all of my friends and family.

Understanding that, Weaver wanted a device that he could hand his daughters, which would, out of the box, have the privacy they need, and to which they have a right. And their friends could get one. And so could their friends. Everyone who wanted to communicate privately and securely could do so. Weaver's idea is to make privacy and security as easy as surveillance. Just like you buy an Android or an iPhone and start using it to be spied on, you could buy a Librem 5 and not be spied on.

Recognizing that smartphones — by the nature of their various sensors and chips — are practically designed as surveillance devices, Weaver decided to create a smartphone that respects users' digital rights. "The primary problem [Purism seeks to solve] is digital rights," he said, adding, "But the root of that is the devices that people use, and obviously the smartphone is the number one device that the majority of people are using." Weaver went on to say that the smartphone "also happens to be the hardest [device] to solve from the perspective of having a device that respects you, meaning [that] you can own it properly." By "own it properly," Weaver means that you control the device and the flow of data coming in and out of it, since data ownership is inseparable from liberty. After all, if you cannot choose who sees your e-mails, texts, calendar, GPS location, and other data, can you really be said to be free?

Creating a phone "that respects you" and that you can "own" meant the phone could not run a proprietary operating system, since the code could never be verified as being free from spyware. It also meant that the hardware — all the way down to the CPU — had to be open source. It meant installing hardware kill switches to cut the power to the WiFi/Bluetooth and camera/microphone so that users could know for certain that their phones were physically unable to spy on them when those functions are turned off. It meant the phone would have to ship with apps for private, secure communication and allow users to install other such apps.

In August 2017, Purism launched a 60-day crowdfunding campaign to raise $1.5 million to begin development and create the Librem 5. Partly because of increased public interest in the wake of not only Edward Snowden's revelations, but also reports of the surveillance being routinely conducted by Google, Facebook, and other Big Tech companies, and partly because of Purism's record for delivering on promises, the goal was exceeded by 78 percent. Purism raised almost $2.7 million and is now shipping early versions of the Librem 5 to those donors.

The Librem 5 runs a Linux distribution, called PureOS (the same operating system that runs on Purism's laptops) created by Purism. When coupled with a USB hub, keyboard, mouse, and monitor, the phone will double as a desktop computer replacement — a goal even Microsoft failed to realize.

Everything about the Librem 5 (including the design schematics) is open source and freely available from Purism, allowing verification of Purism's claims about the device. The CPU contains no mystery code. And putting both hardware kill switches in the off position also cuts the power to the radio the phone uses to communicate with towers, as well as the GPS chip.

And while the baseband (that radio that communicates with mobile towers) does include some proprietary blobs (since there is currently no way around that), the Librem 5 is the only phone that keeps the baseband separate from the CPU. All of this adds up to Librem 5 being the only smartphone (at present) that qualifies for the difficult-to-achieve "Respects Your Freedom" certification from the Free Software Foundation.

Written by **C. Mitchell Shaw** on January 20, 2020

Published in the January 20, 2020 issue of the New American magazine. Vol. 36, No. 02

Decentralized Services for Greater Privacy and Freedom

As to his commitment to open source protocols for interoperable, privacy-friendly services, Weaver has put his code where his mouth is. Librem One — a full suite of secure, encrypted services including Librem Mail, Librem Chat, Librem Social, and Librem Tunnel (VPN service) — is now available and can be used on the Librem 5 and other phones to allow users alternatives to Big Tech's "digital jail" model of services.

Librem One's services are all built using open source protocols. This means that no one is locked in or controlled when using these services. It also means that someone using one of these services could communicate with anyone using another service that was built to that same protocol. If, for instance, User A is using Librem Social (built on the Mastodon protocol for decentralized social media) and user B is using another service built on that same protocol — such as EagleFireNation — they would be able to find each other and connect. No "digital jail." As services such as these compete with Facebook, Google, and other Big Tech services, that competition could lead to a shift in societal expectations of what is acceptable where privacy and other digital rights are concerned.

As implied above, Purism is far from alone in its quest to decentralize the Web in general and services in specific. And while Purism focuses on both endpoint devices (computers and phones) and services, other companies are keeping their focus on only services. EagleFire — based in Ohio — is using decentralized, open source protocols to create services similar to those offered by Purism. This means there is competition in the digital-rights-respecting marketplace, so users have a choice.

Scott Andrews, founder of EagleFire, told *The New American* that he started EagleFire because, "coming from a Big Retail technology and marketing background, I saw firsthand personal data being collected and what was being done with it" and was "appalled." As to the relationship between liberty and privacy, Andrews said, "First let's understand the fundamental principle that truly empowers online privacy: personal data is our property. We have inalienable ownership rights to personal data just like our other God-given liberties. EagleFire provides personal data ownership first and privacy as a natural extension of that ownership."

EagleFire does that by providing dedicated hosting of essential online services and dedicated data storage to each customer, which gives the user greater control of his data. By having dedicated storage of personal data, the customer has decentralized services provided along with full control of his personal data. Customers also get to track by whom, when, and where personal data has been accessed and can change those privileges when they want.

As to how decentralized services such as those offered by Purism and EagleFire differ from the centralized services so common in the digital space today, Andrews explained, "Decentralization of online services is the only way to achieve personal data ownership and privacy." Why? "Centralized services, such as Facebook, collect personal data into one place and share storage space among accounts/subscribers to streamline costs and increase profits. That is a recipe for privacy issues, massive data breaches, misuse for political reasons, etc." Andrews went on to say, "By decentralizing online services and providing each customer their own suite of services, only they can control them and thus have full property ownership rights over the data those decentralized services collect."

These decentralized services serve as competitive alternatives to the monopolistic "locked in" services

of Facebook, YouTube, etc. By respecting the God-given digital rights of users to own and control their data, these services already offer something Big Tech doesn't offer. If such services catch on, Big Tech could find itself in a position where it may have to shift its model to stay competitive. Even if Big Tech holds to its current model, users will have more and more choices as freedom-respecting protocols continue to catch on.

As Web 3.0 continues to come online, the services and products offered by Elix-xir, Inrupt, Purism, EagleFire, and others appear to be just in time to empower users in a "digital rights/data ownership" revolution. Given how broken the Web is, the vision of these few pioneers to steal it back from Big Tech is lofty indeed. But then, so was the vision to create the Web in the first place. All in all, the future of the Web is looking up. If users, equipped with these tools, are able to wrest control from the grasping clutches of Big Tech, the Web may finally be a free place once again.

Photo credit: AP Images

This article originally appeared in the January 20, 2020 print edition of The New American.

Written by **C. Mitchell Shaw** on January 20, 2020
Published in the January 20, 2020 issue of the New American magazine. Vol. 36, No. 02