In Defense of the Private Web – Key to a Non-Totalitarian Future

"The private web could and should be the locus of normal on-line retail."

By Jonathan Carriel

Very recently, it's been dismaying to hear some respected libertarian/anarcho-capitalist pundits – usually intrepid optimists – speak with grim pessimism about the perceived "inevitability" of Central Bank Digital Currencies ("CBDCs"). CBDCs are electronic fiat exchange units intended to function on a blockchain with the convenience of cryptocurrencies, but which completely wreck the impetus of freedom that drove the cryptos' original creations. CBDCs would be digital tokens for the existing national fiat currencies, which would soon be proclaimed "legal tender."

CBDCs could become the ultimate cash-destroyers. They could be distributed on plastic cards to a nation's entire population (doubtless with some free "helicopter money" attached in time for the next election). They would be forcibly merged with any bank, brokerage, or credit card account a citizen had, and cash – paper money and coins that could still be privately exchanged – would be phased out.

This would all be done ostensibly to benefit the public. There's no question that internet-based value exchanges are fast and convenient. They are already very popular. So what could possibly go wrong?

Every exchange made by every individual would be monitored by politicians, that's what. Algorithmic programs would call bureaucratic attention to any exchange that failed to merge with the priorities set by the government. The population would be watched for any purchase that deviated from politically fashionable norms. This would eventually descend to the level of the current Chinese "social credit system," which also employs facial recognition programs to monitor public behavior, or even below that, to enforce an absolute equality of all humans in all respects. (Sparing the "vanguard," of course.)

The pessimism expressed comes from the clear fact that the majority of people would not see this catastrophe coming until it was too late.

But the pundits are missing out on a positive alternative.

Technology can come to the rescue when ideology fails. This has happened before. The Renaissance was well under way in monasteries and universities, but it was moveable type and the printing press that turbo-charged it. Enlightenment ideas were rife for decades before the steam engine and the industrial revolution liberated masses of people from poverty.

The technology needed today to prevent omnipotent totalitarianism is already here, but it's new and still as rough as a Gutenberg press or a James Watt prototype engine. It also faces intense elitist opposition, just as those advances did centuries ago.

It's *the technology of privacy*, which is built on private-key cryptography, the technique of global decentralization, and the internet itself.

The first – and still predominant – application of the technology of privacy was secure internet communications. Some privacy devices may have been funded to ensure military impregnability, but they were quickly repurposed to preserve universal *freedom of speech*, especially that of independent news sources, such as whistleblowers.

Freedom of transactions via the internet was the application that inspired the invention of bitcoin and its blockchain, and most of the other cryptocurrencies.

Both privacy applications are as yet fully employed only by a minority of internet regulars. These things take time.

A promising, even more recent internet technology, one that faces disfavor amounting to demonization today, is **the private web**.

The private web is those websites that are nearly impossible to trace to any geographic location, any Internet Service Provider, any specific computer – and therefore, to any individual *person*. (Every website on the regular "clearnet" web resides on a computer's hard drive somewhere, and that computer communicates to the internet via its unique Internet Protocol ("IP") Address, the coding of which leads – once the ISP's arms have been twisted – to its owner.)

The private website application was developed by the TOR Project, which is best known for its TOR Browser, which presents the internet in familiar fashion, but encrypts all requests, all addresses, all communications, from the originator to the object website, and back (via additional "hops," or transferring machines, each of which knows only its previous and next step). This makes it horrendously difficult for private or public snoops to eavesdrop on the interests and business of others.

The general presumption of the World Wide Web has always been that anyone creating a permanent "address" on the web would *want* all others to be able to find it. Thus, a public Domain Name System ("DNS") was created to direct internet traffic expeditiously via the Universal Resource Locator ("URL"), the humanly readable "address" of the site. All well and good – *except* that this system also permits those private and public snoops to easily monitor all traffic, and to physically locate both parties to the interchange.

The TOR Project's private web enables communications via a different mechanism:

- The IP Address of the website is held only in an encrypted database privately maintained by the Project.
- It issues a unique URL on request, which consists of 56 non-memorizable gibberish characters, followed by the ".onion" extension. The public DNS has nothing to do with it, and so a private website cannot be found through such conventional search engines as Google. (Private web URLs must therefore be privately obtained. Private website addresses are distributed at the *option* of the website owner.)
- Lastly, a private website can only be reached by using the TOR Browser, which ensures that all parties communicating with the website are protected against eavesdropping, and the activities of one party cannot lead to awareness of the others.
- [Note: TOR (which stands for "The Onion Project" – because it works as a set of layers, each of which knows only its neighbors, you see – calls its private websites "Onion Sites." The premier program that creates them, introduced in 2014, is called "OnionShare."]

All of this sounds complicated. It *is* somewhat tricky, but a basic private website can actually be situated on an ordinary home personal computer. Both the TOR Browser and the private website program are free of charge.

Many large businesses, especially news organizations, maintain private websites to enable whistleblowers to submit evidence of wrongdoing without threats of retaliation. Advocacy groups use them to protect members, contributors, and contacts. Many individuals and organizations use private websites simply in the name of preserving their privacy.

A *major* potential use of the private web, not yet explored, is to enable regular private *transactions*. Should CBDCs be inflicted on your country, and followed up with some faction's notion of social credit, perfectly ordinary transactions will quite possibly raise bureaucratic eyebrows, become dangerous, become illegal, become *criminal*. The more difficult one makes surveillance technologically, the less one needs to rely on reasoned moral argument and political activism to counteract this threat. (Please understand that reasoning and activism are *not* being disparaged, only supplemented.)

The original idea of cryptocurrencies was to make private transactions *private*, free of surveillance, bureaucratic oversight, and political interference. But cryptocurrency transactions, like banking transactions, are conducted over the clearnet, subject, albeit with some effort, to private (criminal) and public (bureaucratic) obervation and interference. It took the politicians several years to realize that cryptos threatened their hold on the money spigot in any way, but they are now in a rush "to protect the public" from illicit transactions such as getting one's hard-earned savings out of their reach.

The private web has the potential to be a truly free universal marketplace. Someday the majority of the public should today be able to transact the majority of their purchases – both ordinary and controversial ones – without fear, on the private web.

Why has this not happened already? Several reasons – some obvious, some not.

- Even in the well-to-do world, many are still new to computers, to the internet, to on-line transactions of any sort. The "friendliness" of new, constantly-improving softwares is a great continuing challenge not only to most users but to most developers.
- Like a Ford Model T of 1918 (ten years after *its* first introduction), the private web may be a wondrous modern marvel, but it is not nearly as uncomplicated – or as robust – as its consumers could desire.
  - A fascinating recent article by "bad cattitude" presents a completely different approach to the problem, involving steganography and a new structure to the internet.
- There have been a few well-publicized cases where the private web has been breached, usually thanks to simple user error – and even then only with terrific difficulty and a major expenditure of taxpayer funds.

But the chief reason regular transactions have not migrated to the private web is, of course, the fact that it has been viciously *demonized* by the authoritarians, from the first moment they realized that private on-line transactions could not only evade regulations, they could evade taxation. Wikipedia repeats some 2016 "reports" asserting that 56% of all private web usage is "illicit." The private web – generally still known as the *hidden* web or, worse, the *dark* web – has been deliberately associated only with transactions that most people, even those who might believe some of them ought *not* to be illegal, would still regard as morally repulsive. One can confidently say that even today, good readers of this article could browse most of the retail outlets of the private web – recommended for a quick education – and find only products that are, at best, silly and useless, down through goods of no personal interest, to stuff that is truly repugnant. Given this situation, many people fall for the constantly reiterated suggestion that just touching the private web could taint them for life.

I don't doubt that some of the money being exchanged on the private web is ill-gotten. But I would imagine that the proportion of “dirty” money being laundered to innocent life savings being rescued … is roughly the same as the proportion of honest humans to criminal ones. The insidious purpose of Anti-Money-Laundering (“AML”) regulations is to besmirch all attempts to exchange failing or threatened fiat currency into anything more solid. The result is a great injustice and a squandering of personal and societal capital.

But why does this *have* to be the case? **It doesn’t.**

The private web could and should be the locus of normal on-line retail. As the public finds government ever more intrusive into their individual choices, the private web should become a preferred option. Increased use would encourage friendlier software and sturdier infrastructure, and privacy may eventually become everyone’s default choice.

Given the current status, however, there doesn’t seem to be much anyone can do to speed this process up. **But there is.**

- Anyone using a computer can download the free TOR Browser to enhance their privacy on the clearnet. In time, they can explore private websites, perhaps first concentrating on informational and advocacy offerings.
    - Various “apps” can be found that emulate the TOR Browser on mobile phones and tablets.
- Computer users with basic HTML (the website creation “language”) can create a free site to transfer files of any description to interested parties world-wide, using TOR’s free *OnionShare* option.
- Anyone who already *has* a website – whether retail is involved or not – can fairly easily and cheaply simply *duplicate it* exactly on the private web, giving readers the option of browsing it there.
- And of course, being a not-for-profit organization, the TOR Project is glad to accept contributions.

The more common use of the private web becomes, the more that normal retailers will be emboldened to offer it as an alternative.

In addition to libertarian ideology and free-market economics, the developing technology of privacy – already available through the internet for both communications *and transactions* – is our chief hope for a non-totalitarian future. While challenges and pitfalls of all sorts can be expected along the way, an optimistic creed holds that human decency and ingenuity will *out-think* the scoundrels in the long run.

Jonathan Carriel [Send him mail] is the author of the Thomas Dordrecht Historical Mystery Series, but he is currently developing the **Bedrock Digitized Bullion System** [clearnet site – private web site], a business concept that would merge the solidity of precious metals with the exchange capability of the global cryptocurrency market. A long-time New Yorker, he now lives in Panama City, Panama.

[Published May 18, 2024]