Communications Under Tyranny

by Jim Davidson
jim@resilientways.net

"If privacy is outlawed, only outlaws will have privacy."
~Philip Zimmermann

Rape Survivors

Many long years ago, when the Internet was newer and less infested with communists, there were people who wanted to talk about their experiences without giving their names. Also in that era, there was a guy named David Chaum who wrote a paper (1981) that proved it was possible to have anonymous communications with both the content and source of the content obscured through open source cryptography then known and understood in the tech community. Also in that era, there was a Finnish hacker named Julf who set up an anonymous remailer called anon.penet.fi which became useful to many people.

It would be incorrect to say that the entire point of these exercises was to help rape survivors talk about their experiences without being further attacked by the rapists who raped them. It was my experience, though, that the arguments made by rape survivors about how important this capability was to them that were among the most compelling. I was convinced, in part, because of my own need to be able to speak about past experiences without being confronted by some of the people involved. Rape survivors benefited from these tools and technologies as they became available. And, of course, it is important that rape survivors be free to tell what happened to them and to discuss the things they endured in order for them to have the opportunity to heal from the trauma of what was done.

In some ways, when you consider interactions with the state, everyone on Earth is to a greater or less extent a victim of coercion, the threat of force to get an unwilling party to do something that the assailant wants. Yes, I am saying that human governments are rapists, both literally in the sense that there are many places including in the United States where the police are rapists and wife beaters and murderers and get away with violence without being held accountable, and also figuratively in the sense that all taxation is theft and all enforcement by governments of human-made laws is akin to rape.

Secret Codes

News flash. Secret codes not only don't work, they don't stay secret for very long. I mention this point because I am at times asked to work with someone using a code they have devised. Then they share the code, and I'm, "Oh, well, gosh, now everyone knows." Code breakers used to rely on really artful tricks like capturing an enemy merchant vessel and reading the code books in the captain's safe. Or sinking a submarine and then recovering the mechanical cipher device used to encode and decode messages.

Secret codes proved to be vulnerable to all kinds of techniques for learning the secrets, as well as vulnerable to all sorts of techniques for breaking the codes. So better ways were wanted. And what ways were found? Well, many coders were good at mathematics and there are some really interesting mathematical operations that are easy to perform and hard to undo.

For example, you can multiply two numbers together really easily. If you do that with a computer, it can take less than a millisecond. If the two numbers happen to be prime numbers, and have many digits, and you want to undo that operation without knowing which two numbers were used, you have a

very difficult problem. Factoring a number into its prime numbers is not easy. The more digits in the prime numbers, the harder the task.

Secure Communications
Students of military history can give numerous examples of situations when one side had more secure communications than the other side. I do not know of any instances where the side with insecure communications was victorious, and I can think of any number of examples of information falling into the hands of the enemy causing battle plans to go awry. The battle of Sharpsburg, for example, also known as "Antietam," and probably the single worst mass shooting event in American history, would have gone very differently if a copy of General Lee's orders for the movement of his forces was not "found" by some Union troops wrapped around some cigars. Or, if that document had been encoded at all, the outcome would likely have been very different. Arguably, Lee could have captured Washington DC and ended the war.

Another example that has become fairly widely known is detailed in Robert Stinnett's book "Day of Deceit" and in other books. The codes of the German military, especially the Enigma mechanical cypher machine codes, were broken early in the war. The Japanese military codes were also broken, as early as October 1940. The fact of these codes being broken was kept secret, and the intelligence gathered from reading the enemy's messages was very valuable to the war effort. Also, as it happens, the information was not shared widely even within the American military, and as a result the "sneak" attacks on Pearl Harbour and the Philippines and Batavia (among other places) were much more damaging than they would have been had suitable preparations been made.

It is a fact that secure communications are important, and that means, today, encryption technology. It is also a fact that "proprietary encryption" means you are being deceived.

Ersatz Privacy
Over the years, many people have told me that they are "on Skype" and that I should "get on Skype." I have always refused. Skype, whenever I've looked into it, does not use end-to-end encryption, and allows for "routine" monitoring by Microsoft and by USA government agencies.

Software that **does** provide end-to-end encryption and uses open source protocols so that the effectiveness of the encryption can be verified and tested is often attacked in publications that pretend to cover the tech industry. As a result, it is often difficult to be sure what is and is not being done behind the scenes by "apps" to keep your information private, or to compromise it and make it available to bad actors. Yes, I'll go ahead and say that I believe Microsoft and USA government agencies are evil, violent, involved in mass murder and mass enslavement, and are to be avoided.

Free Software
Long enough ago that it has slipped down the memory hole for many, a guy named Richard Stallman came up with the term "free software" to describe software that was not proprietary and that did not keep its source code from the public. Over time, the idea came to be embraced by a great many innovators in the tech community. When Netscape began to consider a "free software" approach to its code base, the term "free" was considered a difficulty to the investors in the project. Christine Peterson of the Foresight Institute coined a new term "open source software" which is still used today.

I'm old enough to have met K. Eric Drexler and Chrstine Peterson in 1982 at a lunch in the Boston area when I was seeking permission from the L5 Society to form a joint chapter of L5 and the Planetary Society at Columbia University. The lunch was a success. The chapter was not.

Over the years, an increasing amount of software, including operating system software, has been developed as open source software. Which means that the entire community of active software coders, now several tens of millions or people worldwide, along with anyone who can read and understand software code (perhaps hundreds of millions) can see the source code, understand what it is doing, and be aware if it does unreasonable things like sending a copy of your hard drive to a government agency.

If you are using a proprietary operating system for your computer, you are never going to know what it is actually doing. If you are using proprietary software applications, you are never going to know what those apps are doing. And if you want to have any privacy, any freedom, and any opportunity to free the slaves and stop the wars, well, my friend, you need to ditch the bad code.

Cell411

One of the apps that I've been asked to work on recently is called Cell411. Its purpose is to connect people who are willing to help one another into "cells" so that when someone is in trouble they have an alternative to calling the governmental authorities. Instead of dialing 911, which is a recipe for death, a person with an emergency can pick up their smart device, or go to their computer, and hit an "alert" button. That alert goes to people chosen in advance who you want to notify in case of emergency.

The Cell411 app can share with them your location, even if you become incapacitated. It can, of course, be *prevented* from sharing your location information if you want to set it that way. The Cell411 app can help you be in immediate communication with a group of concerned people, your "cell" who get information ("the 411") about what is happening, and who can come help you, or send help as they think best.

As well, the Cell411 app can stream video and even upload that video to servers so that what is happening can be documented in real time.

Given that you now live in a world where the governments are all against your freedom, prosperity, and privacy, it is well to consider not relying on the government to help you. Given the very large number of Americans who are arrested every year (about 10.08 million in 2019, according to one report) and given that about 4.9 million are jailed every year, often in very dangerous conditions, often subject to rape and violence while in custody, it is unwise to "trust" the government.

CopBlock.app

Another app project on which I've been asked to work is CopBlock.app which is being re-developed using the Cell411 technology. The purpose of CopBlock is to make it possible for people to observe, video, and report on the actions of the police in real time. The intention is to allow the 330 million Americans who are harmed by, frequently attacked by, and restricted by the 690,000 law enforcement officers and sheriffs deputies in America to keep tabs on what those violent, vicious, murdering rapists are doing.

Why? Because knowledge is a form of power, and knowledge about the misdeeds of corrupt violent people can be used to warn others, possibly gain some redress in the courts, and certainly give bad actors reason to limit their bad actions.

Mesh, Ham, and Other

If you are concerned about the Internet being vulnerable because, for example, the root name servers are significantly centralised, and because some domain registrars are statists, you may be interested in

some other technologies. Way back in 2006, my friend Venkat Manakkal and I presented a paper on self-extending wireless networks using a micro-payment system in a digital currency. At the time, it was to be a digital gold currency then being developed by Venkat and some of his associates, including me.

Today, of course, you'd describe the same concept as a "mesh network" and you'd be using the best crypto-currency for the job, whether sharding or otherwise, because that's essential when you're talking about processing micropayments in nanoseconds to avoid bogging the routers.

Another technology that works around the issues of centralisation that some find concerning is ham radio. Ham is not an acronym, it refers, as legend has it to "ham fisted" telegraphers whose Morse code was hard to understand because of low skill. Ham radio is amateur radio, and there are a lot of devices you can get for that purpose, even without a licence. Indeed, most equipment is sold in most of the world without a licence, and even in the United Kingdom, many people own receivers without licences.

Your approach to technology could also include IPFS and other innovative technologies that allow for a completely different "browsing" experience. IPFS stands for "interplanetary file system" and is a technology suite developed specifically to enhance the safety and freedom of the internet. More information here and in recent project documents I've seen.

Your Help Please

We're developing a business plan for making these apps better, for deploying them, and for realising the economic potential of related apps for things like ride sharing, room rentals and couch surfing, dating, and free market exchanges, including "agorist delivery" services for those in the "agora" - the Greek word for marketplace. We're developing, with volunteers presently, patches to the code base of Cell411 and planning new releases soon. In fact, a patch for many of the recent problems with Cell411 is being tested right now. Also in the works, we'd like to engage some web developers to rebuild and update the Cell411 web site and the CopBlock.app web site.

We'd like to be able to continue to provide the best services possible, with fast servers, great software, and new versions to fix problems as they arise. We'd also like to let people far and wide know about our apps and their uses. We'd like to have your help, through donations or through volunteering time, and ultimately we'd like to have a going concern that is funded from revenues brought in from related apps as discussed above.

Would you please help? If you don't know the people who are involved, please feel free to contact me and I'll put you in touch with them.

Free the slaves. Stop the wars. End the state. You'll be glad you did.

=======

Jim Davidson is an author, entrepreneur, actor, and director. He is the vision director of **HoustonSpaceSociety.net** You can find him on **Twitter.com/planetaryjim** as well as **Pocket.app** and **Flote.app** also as planetaryjim. He appreciates any support you can provide as times are very difficult. See the Paypal link on this page. Or email your humble author to offer other choices. This week Jim learned that **SubscribeStar.com/planetaryjim** is working, so he'll be adding new things there soon. Visit **IglooLuau.com** for more information. Those seeking a multi-jurisdiction multi-hop VPN for communications privacy please visit **https://secure.cryptohippie.com/houstonspacesociety.php** For those seeking colloidal silver try **ppmSilver.com/Jim** Ask Jim about CryptoWealth. Coming soon: FreedomLandDAO.com - under construction. Just arrived: **FreedomDeFiSoftware.com**