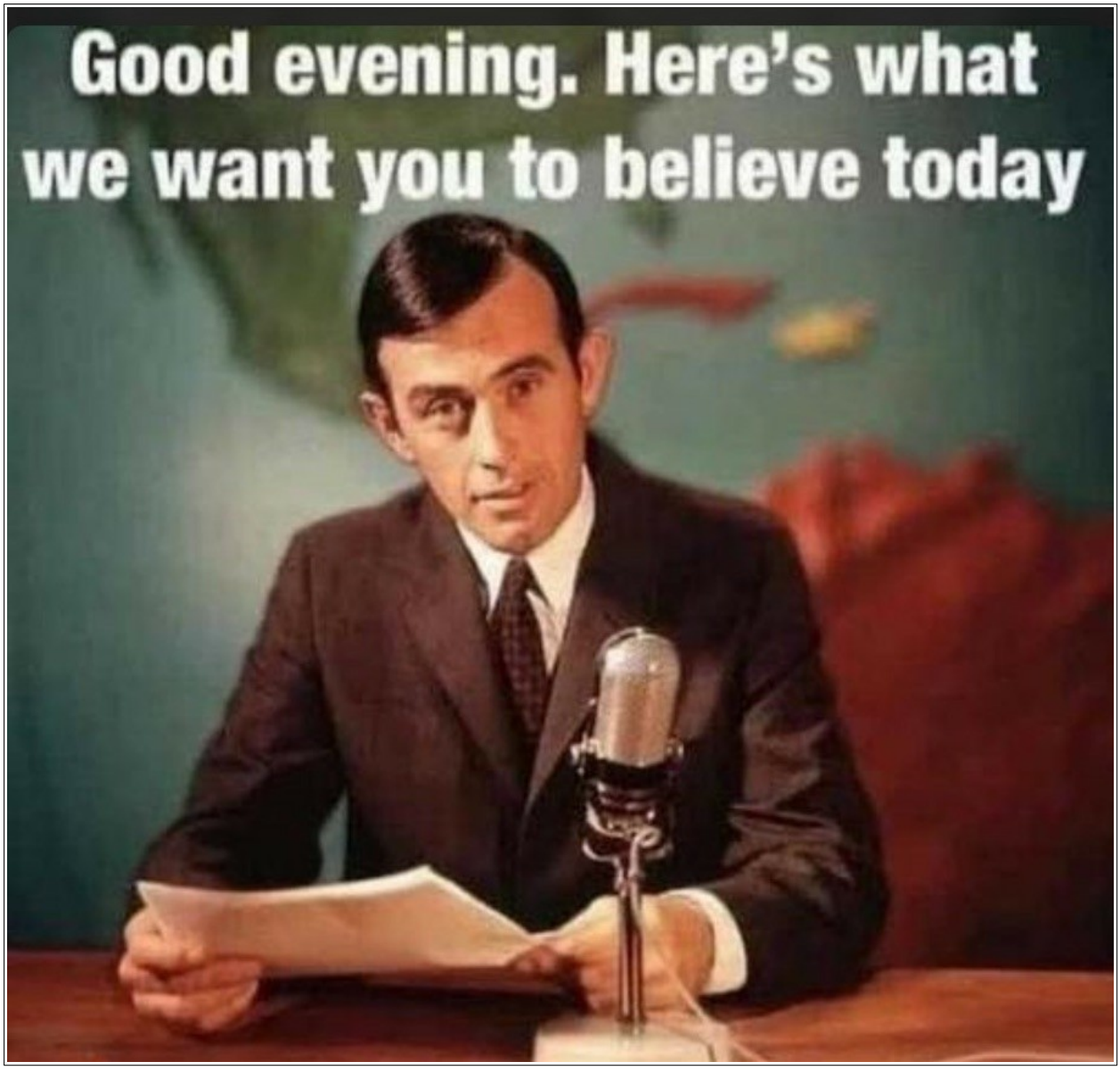
Anonymously and Securely Accessing Digital Information



TnT Net, Hosted by 11 Cats, 30 March 2024

Table of Contents

Introduction

Approximately 20 trillion dollars of debt ago (~2004), a senior White House official allegedly stated: “We're an empire now, and when we act, we create our own reality. And while you're studying that reality—judiciously, as you will—we'll act again, creating other new realities, which you can study too, and that's how things will sort out. We're history's actors...and you, all of you, will be left to just study what we do”.

Now, 20 years later, we are not just studying it, we are living with it. The imaginative minds of the era knew as previous administrations did, that they could push fiction as facts to achieve whatever public support was needed for otherwise career terminating actions and policies. However, decision and policy makers of the era underestimated how the world would use the Internet. While previous administrations had a manageable number of media outlets to deal with, they did not have to deal with a global population using the Internet to collaborate and share information. Information freedom rocked a domestic and international data collection, surveillance and control system that had been in place for over half a century and posed a far greater threat than the Church committee investigations did in the 1970s. Information freedom posed a significant threat and diminished the ability of the mainstream media to establish and maintain a coordinated narrative.

The decade saw growing pubic distrust of government and institutions while feeding a growing bureaucratic paranoia. People working together against the goals of those pulling the strings of government, as they did for a short time during Occupy Wall Street, led to HR 4310. HR 4310 ended the ban on domestic propaganda and opened the doors for psychological warfare techniques to be used against US citizens and residents, establishing a legal foundation for total information control (officially Total Information Awareness, TIA).

Allegedly under TIA, the ends justify any means necessary to achieve them. Ask yourself if the program has been effective? Investigative journalism is dead, professionals such as doctors must obey or risk losing their licenses, censorship, divisive media narratives, effective and in some countries legally enforced irrational groupthink: I*t is only fair that men who claim they are women must be allowed to compete with natural women. Men can have babies and breast feed. An allegedly educated woman who could not define what a woman is. It wasn’t his notebook – then it was, but Russia tampered with it (lol, gets funnier each time it cycles through the media machine). Equity over equality. Intentionally divisive reporting, etc.*

The irrationality is entertaining. However, paraphrasing Ayn Rand, “You can ignore reality, but not the consequences of ignoring reality”, leads one to ask, **What is our reality today?**

One example is this writer, I am typing this near the St. Louis Airport. Access to some of the reference material was blocked by the Internet Service Provider (ISP). I was able to use the Tor Browser to collect the current information I needed to complete this paper.

So, how can we we determine reality outside of direct observation and measurement? When some governments, corporations, alleged academics and scientists get caught cherry picking data, modifying historical records, falsifying articles in professional journals, blackmailing or eliminating critics, etc. so a leader may say with a straight face that their policies and legislation are based on "science". When formerly prestigious news organizations choose to report the same opinions and alleged facts across the board, with often the exact same sentences! LOL When government and corporate officials believe that they, and only they have the right to label what is true, what is false, what is mis-information (1), what is dis-information (2), what is mal- information (3), regardless of accuracy and truthfulness?

Where can we review data and conclusions that have not been "Corzined" (from the MF Global, "poof" it's gone fiasco) anonymously? Mainstream media news and entertainment has turned into nothing more than a propaganda and psychological warfare tool. The public internet today is a conflicting cesspool of irrational ideology and alleged "facts" that change to whatever the woke mob demands. Ham Radio is great but has no anonymity and security. Older printed books cannot be modified by Department X and while they are excellent reference material, they do not provide current information.

These considerations have led to the development of protocols and systems designed to provide anonymity and provide secure bi-directional information flow.

WARNING: Mainstream operating system and communication vendors have allegedly been forced to partner with the USSA alphabet soup under Section 702+(4) to continuously search cloud data and devices as well as provide historical and on demand real time surveillance. The Snowden and Vault7 dumps expose the operational tip of this iceberg. Improper and/or careless use of these tools may result in a publicly funded vacation at best, a Seth Rich experience at worst.

Tools for anonymity and data transport security

Tor Project

The TOR Project [6] provides TorBrowser. Tor Browser is a Firefox based browser preconfigured to access the TOR network. The browser provides three security levels (Standard, Safer, and Safest). The browser blocks trackers, defends against ISP surveillance, resists fingerprinting and provides multi-layer encryption. The DuckDuckGo onion search portal [7] is one place to start searching.

Tails

TAILS [8] is a complete Linux Debian operating system that boots from removable media on your computer. It offers secure removable storage and provides the TorBrowser and a good selection of applications and utilities.

Kodachi

The Kodachi [9] operating system offers a highly secure, anti-forensic, and anonymous computing environment. It's designed with privacy in mind, incorporating all the features needed to maintain user confidentiality and security. With a straightforward setup process, Kodachi is user-friendly and doesn't require any Linux expertise. Simply boot the system from a USB drive, and you'll be up and running with a fully-operational operating system. This includes an automatically established VPN connection, a pre-configured connection, and a running service, all optimized to maximize your online security and privacy.

I2P

I2P [10], also known as the Invisible Internet Project is a fully encrypted private network layer that protects your activity as well as your location. All I2P traffic is internal to the I2P network and does not connect with the public Internet directly. I2P offers resistance to pattern recognition and blocking by censors.

Freenet

Freenet [11] lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums without fear of censorship. Freenet is decentralised to make it less vulnerable to attack and if used in "darknet" mode, where users only connect to their friends, is very difficult to detect. Communications by Freenet nodes are encrypted and are routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is. Users contribute to the network by giving bandwidth and a portion of their hard drive (called the "data store") for storing files. Files are automatically kept or deleted depending on how popular they are, with the least popular being discarded to make way for newer or more popular content. Files are encrypted, so generally the user cannot easily discover what is in his datastore, and hopefully can't be held accountable for it. Chat forums, websites, and search functionality are all built on top of this distributed data store.

Cubes and Whonix

Cubes [12] allows you to isolate different pieces of software as if they were installed on separate physical machines using advanced virtualization techniques. Whonix [12] is a free and open-source desktop operating system (OS) that is specifically designed for advanced security and privacy. It's based on the Tor anonymity network, security-focused Linux Distribution Kicksecure™, GNU/Linux and the principle of security by isolation. Whonix defeats common attacks while maintaining usability.

Conclusion

Many tools exist that can enhance your ability to access and review information. No tool is perfect. Securing data at rest is as important as securing it in transit. Be careful and alert and for important investigations - buy random with cash. Consider only using a machine that can be wiped at the conclusion of an investigation. Do not use any of your standard logon credentials on your research machines and store no personally identifying information on your research devices. When not in use keep them powered off and ensure all auto-wake triggers are disabled. Scramble firmware serial numbers and MAC addresses. Check all privacy settings after software and firmware updates.

For more information, please consider reviewing personal security articles at https://www.eff.org

Notes

1. Mis-information is simply inaccurate information and is classified as unintentional. It's often used as a descriptor for all kinds of falsehoods and may result from an error, cognitive bias, or laziness in fact-checking.

2. Dis-information is classified as inaccurate information conveyed deliberately—with the intention to deceive.

3. Mal-information is classified as both intentional and harmful to others.

4. Section 702 of the FISA, Foreign Intelligence Surveillance Act

5. EFF: https://www.eff.org
   EFF Tor: https://www.iykpqm7jiradoeezzkhj7c4b33g4hbgfwelht2evxxeicbpjy44c7ead.onion/

6. TOR Project: https://www.torproject.org/

7. DuckDuckGo Onion:
   https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/

8. TAILS Project: https://tails.net/

9. Kodachi Linux : https://www.digi77.com/linux-kodachi/

10. I2P Project: https://geti2p.net/en/

11. FREENET Projectt: https://staging.freenetproject.org/pages/download.html

12. CUBES Project:
    https://www.qubes-os.org
    and WHONIX Project:
    https://www.whonix.org