

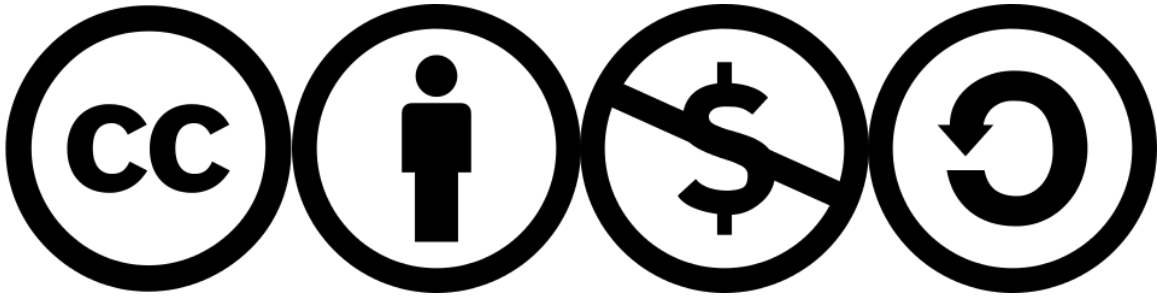
Just Below the Surface

A Guide to Security Culture

By Kyle Rearden

Foreword by Shane Radliff





This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-nc-sa/4.0/). Any other content within this work that may not be covered by this CC-BY-NC-SA license is hereby used under the intention of [Fair Use](#).
No copyright infringement intended.

Table of Contents

Foreword page 6

A Primer on Security Culture page 7

Section I: Telecommunications

A History of Dragnet Wiretapping page 12

Data-Mining the Haystack: Should You Attempt to Overload the NSA's Servers with "Suspicious" Email Keywords? page 19

Are Cellular Telephones Furthering Human Liberty? page 23

Dual Layer Encryption: A Proposal for Sidestepping Potential Backdoors page 36

How to Configure & Use PGP Encryption for Email page 39

How to Configure & Use Jitsi (Windows OS) page 53

Section II: Information Security

Socialist Insecurity: How the Raw Deal Enslaved Americans page 59

Do You Have the "Right" to be Forgotten? page 76

<i>Sifting the Wheat from the Chaff: The Value of Skepticism</i>	page 84
<i>Modeling Threats & Analyzing Risk: A Rebuttal Against “Doom Porn”</i>	page 99
<i>The Libertarian Case for Judicial Transparency</i>	page 117
<i>Secured Record Archival: How to Protect Your Documents from the Governments</i>	page 123
<i>Keeping Your Own Counsel</i>	page 135

Section III: Low-Profile Behavior

<i>Chilling Dissent: How Government Demonizes Americans</i>	page 138
<i>Fanciful Notices: Should You Post a Warning Sign on Your Property?</i>	page 147
<i>How to Roleplay Police Interrogations</i>	page 152
<i>Blending In: The Art of the Grey Man</i>	page 158
<i>How to Make Your Car Inconspicuous</i>	page 162
<i>Home Hardening: How to Fortify Your Domicile Against Intruders</i>	page 164
<i>Interpersonal Diplomacy: The Value of Keeping the Peace</i>	page 167

<i>Disingenuous Activists! Why Leaderless Resistance is Preferable to Formal Organizations</i>	page 169
<i>You Are Known By the Company You Keep: How to Choose Your Allies Wisely</i>	page 175
<i>May You Live in Interesting Times...</i>	page 180
Afterword	page 183
Bibliography	page 184

Foreword

Kyle has been a major advocate and pioneer in the field of security culture, ever since I made his acquaintance in March of 2015. His knowledge and advice on the subject led to my advocacy and practice of this strategy where I am able to in my own life. I use encryption, I have role-played police interrogations (and have even utilized those skills in encounters with the bludgies; aka, police extortionists), and I act as the grey man whenever I am able.

That said, the practice of security culture has never been more important. Having archived the court documents for over 30 political prisoners, I think that alone is demonstrative of that fact, although, there are other examples, such as the life-invasive tools now available to the State in modern times. With even a lackadaisical application, it is safe to say that at least a number of the current political prisoners would still be enjoying the limited freedoms they had left, instead of wasting away as they now are in a government dungeon.

In this anthology, he provides an overall, in-depth analysis of various security measures, such as secured record archival, making your car inconspicuous, home hardening, and much more. Not only does he critique methods already available, he expands upon them and even includes his novel contributions, such as Gary Hunt's proposal of dual layer encryption.

Those who don't know history are doomed to repeat it, and he is fully aware of that fact. So much so, that he provides a historical analysis of topics like Social Security, the blatant failures of activist organizations, and even the surveillance police state apparatus, among others.

He also examines the viability of certain tactics, such as overloading the NSA's servers with suspicious email keywords, as well as the practice of putting up "fanciful notices" informing the bludgies that you are aware of and are exercising your rights. As naïve as those sound (and rightfully so), Kyle's humorous critiques should put those to rest, but I don't see the reformists giving up their "activist" highs that easily.

The overall result of this anthology is yet to be seen, but nonetheless, it is an extremely important, indispensable contribution he's made to the alternative media, as well as anyone else who gives a damn about their privacy.

Before beginning your endeavor, I feel it's important to provide you with a warning. Some of the articles you read may scare you, and that's certainly understandable. The NSA collecting phone calls and metadata isn't even the tip of the iceberg. At times, you may feel violated, but in order to defeat (or defend yourself) from your enemy, you must first know the tactics they are utilizing to spy on every facet of your life, or more broadly, to enslave you.

Are you going to take the steps necessary in exercising your right to privacy? Your answer to that question is more important than you could ever imagine.

Shane Radliff

Bloomington, Illinois

July 2016

A Primer on Security Culture

www.thelastbastille.com/2016/07/05/primer-security-culture/

"I don't accept the idea that if we nothing to hide, we have nothing to fear. Privacy serves a purpose. It's why we have blinds on our windows and a door on our bathroom. Privacy is important to us, it's something that we take for granted as being central to our lives. In other words, we have plenty to hide, and it's always been our right to hide it, until now, because today there are people who don't want us to protect our privacy, who want, and to a large degree, already have free access to our personal information...we have to recognize that both our individual and collective existence depend upon a base level of control over our own privacy. Privacy is not a privilege, and it is not something to be willingly and casually sacrificed. Privacy is fundamental to being a human being, and it's worth fighting for."

— Alex Winter



[Security culture](#), briefly defined, is the direct application of the [right to privacy](#). Some believe that privacy is only valuable insofar as it is relevant to one's survival. This view typically clashes with the ideologically driven perspective that privacy ought to be thought of as an end, a means, and an insight based upon one's principles. What integrates the **privacy-as-survival** and **privacy-on-principle** camps is security culture, which is not only deontologically consistent, but also empirically demonstrative of what happens when individual privacy is respected or otherwise not disregarded.

Why is security culture an application of privacy? The right to privacy is an individual's sphere of activity that is exempted from public scrutiny; similarly, an [expectation of privacy](#) is an individual's assumption that his right to privacy will be respected. In other words, security culture presumes the right to privacy as a given, and as such, is only concerned with how to practically implement it.

Just as important as what security culture *is*, is what it is *not*. [Security theater](#) is the polar opposite of security culture, particularly considering that the latter is the answer to the former. Security culture is not “[civil libertarianism](#),” which is solely reliant upon [legal interstices](#), and even [reformism](#), in purportedly achieving its stated goals of increased human liberty. Furthermore, security culture is also not [survivalism](#), despite some overlap they may share at times regarding emergency preparedness and self-sufficiency.

Properly understood, it should be clear that security culture does not break the government’s laws in and of itself. Although security culture does share with [vonu](#) the desire to reduce one’s vulnerability to coercion, its goal of hardening your life is by no means necessarily comprehensive throughout your lifestyle in the same way that vonu works. Civil disobedience, whether it takes the form of [agorism](#) or [satyagraha](#) (aka, “teasing the bear,” or “falling on your sword”), can be performed in direction violation of security culture, as is often the case. Armed resistance is enhanced by the use of security culture, regardless of the operation’s type (such as [monkey-wrenching](#) or [assassination markets](#)).

Literature about security culture has really exploded over the past two decades. Robert Smith’s [Our Vanishing Privacy](#) (besides his [Privacy Journal](#)), Farren & Gibbs’ [Who’s Watching You?](#), Frank Abagnale’s [Stealing Your Life](#), Bill Kaysing’s [Privacy: How to Get it, How to Enjoy It](#), Claire Wolfe’s [Rats!](#), Gini Graham’s [Mind Your Own Business](#), and Naomi Wolf’s [The End of America](#) have really opened my eyes as to just how wretchedly horrid Leviathan is in exercising raw power. Yet, at the same time, these books have also showed me that all is not lost *if* people are willing to take responsibility for their own actions by stopping their acquiescence to all of these gross invasions of privacy.

Strategically, the use of security culture ultimately leads towards gradually hardening an individual’s life by securing all aspects of it, thereby shoring up anyone’s vulnerabilities from being compromised and exploited. Much like vonu, security culture aims to reduce your vulnerability to coercion, specifically blackmail and extortion. Successful implementation relies upon both the efficacy of tactics as well as their harmonious utilization.

Methodologically, security culture possesses quite a variety to suite a range of tastes. For over three years, I have periodically examined some aspect of security culture so as to discover the truth behind privacy itself. A listed bibliography of the entire series is as follows:

- [A History of Dragnet Wiretapping](#)
- [Data-mining the Haystack: Should You Attempt to Overload the NSA’s Servers with “Suspicious” Email Keywords?](#)
- [Are Cellular Telephones Furthering Human Liberty?](#)
- [Dual Layer Encryption: A Proposal for Sidestepping Potential Backdoors](#)
- [How to Configure & Use PGP Encryption for Email](#)
- [Socialist Insecurity: How the Raw Deal Enslaved Americans](#)
- [Do You Have the “Right” to be Forgotten?](#)
- [Sifting the Wheat from the Chaff: The Value of Skepticism](#)
- [Modeling Threats & Analyzing Risk: A Rebuttal Against “Doom Porn”](#)
- [The Libertarian Case for Judicial Transparency](#)
- [Secured Record Archival: How to Protect Your Documents from the Government](#)
- [Keeping Your Own Counsel](#)
- [Chilling Dissent: How Government Demonizes Americans](#)
- [Fanciful Notices: Should You Post a Warning Sign on Your Property?](#)

- [How to Roleplay Police Interrogations](#)
- [Blending In: The Art of the Grey Man](#)
- [How to Make Your Car Inconspicuous](#)
- [Home Hardening: How to Fortify Your Domicile Against Intruders](#)
- [Interpersonal Diplomacy: The Value of Keeping the Peace](#)
- [Disingenuous Activists! Why Leaderless Resistance is Preferable to Formal Organizations](#)
- [You Are Known By the Company You Keep: How to Choose Your Allies Wisely](#)
- [May You Live in Interesting Times...](#)

Needless to say, the National Security Agency indiscriminately wiretaps telephones without any search warrants because “foreign intelligence surveillance” is an exception to the Warrant Clause of the Fourth Amendment. Trying to overload the NSA’s servers at the Utah Data Center by using emails laden with allegedly suspicious keywords is utterly fallacious simply because you would be using the smallest conceivable file size to overwhelm the largest conceivable set of cloud computing servers. When it comes to cellular telephones, you have no legally effective protections via the Fourth Amendment, so any privacy you can expect to realistically have are most likely to come in the form of an encrypted smartphone using [free and open-source software](#). If you were to blend high-tech cryptographic software with low-tech cryptography, you might very well be able to sidestep any potential backdoors completely; at the very least, you ought to install, configure, and *regularly* use [Pretty Good Privacy](#) in order to encrypt your emails.

Franklin Roosevelt’s [New Deal](#) imposed, among many things, a bankrupt “social insurance” government program that now effectively compels you to keep a vigilant guard over a number that uniquely identifies you. Europeans have tried to scrub the Internet of truthful information about some individuals, and there is demand to import a so-called “right to be forgotten” into America. Wishful thinking and blind faith encourage security theater by ridiculing skeptical inquiry, no matter how full of holes these promoted myths actually are; similarly, the fear-mongering of near weekly “doom porn” seeks to inculcate a sense of [learned helplessness](#) in those who consume the [news cycle](#) like dieters on a binge. Emancipating court cases from the judiciary’s paywall, in order to learn about mistakes that were made by political prisoners when they violated security culture, are cautionary tales warning privacy advocates to take their advocacy as seriously as a heart attack. Securely archiving your records comes a close second to shutting the fuck up about matters you ought not to flap your gums about, especially publicly.

The federal government demonizes Americans based in large part on their chosen ideology, despite being such a flagrant violation of the First Amendment. Posting custom aluminum warning signage is no guarantee that the government police and the judges in their courts will actually respect the limitations imposed by the Fourth Amendment. Roleplaying police interrogations is actually rather quite practical for staying out of jail, yet, blending into the social environment as a grey man is noticeably more preferable. Travelling in an inconspicuous car and fortifying your domicile against intruders reduces the likelihood of harassment and crime against your person and property. Keeping the peace is vital for avoiding unnecessary trouble, as is vetting likely allies and ostracizing disingenuous activists from your circle of trust. If all else fails, the benefits accrued from informant hunting are great should you publicly expose and then shamelessly humiliate them for their proven complicity with the government.

Privacy advocacy organizations, much like the security culture literature, have been popping up in recent decades. Consumers Against Supermarket Privacy Invasion & Numbering ([CASPIAN](#)), the Electronic Privacy Information Center ([EPIC](#)), the Electronic Frontier Foundation ([EFF](#)), Privacy Rights Clearinghouse ([PRC](#)), and even the American Civil Liberties Union ([ACLU](#)) have all spoken out against the rampant abuses committed by the government and their corporations against the privacy of the American citizenry. Much like EPIC and EFF, the ACLU is significant for two primary reasons, namely, transparency and public interest litigation; not only has the ACLU gotten the word out by spreading awareness regarding a plethora of privacy issues, but they also habitually [sue the](#)

[government](#), which although is not always successful or broadly effective, at least it provides a solid basis for expressing one's grievances, if nothing else. ACLU's lawyers involve themselves in matters ranging from [homosexual discrimination issues](#) (including [discrimination against AIDS/HIV patients](#)) to [wiretapping](#), [censorship](#), [government secrecy](#), [cyber-liberties](#), [medical records privacy](#), and [workplace privacy](#).

Interestingly enough, the most valuable advocacy organization, I think, is not one of those who chiefly rely on litigation to make a difference, but rather, informs you of the many and sundry techniques for increasing your privacy using the legal framework as it is right now. PRC has issued "[Fact Sheets](#)" across a range of privacy topics that focus on taking effective action today. I whole-heartedly recommend that you read the following list of fact sheets, at the very minimum:

1. [Privacy Survival Guide: Take Control of Your Personal Information](#)
2. [Wireless Communications: Voice & Data Privacy](#)
3. [How to Put an End to Unwanted or Harassing Phone Calls](#)
4. [Junk Mail: How Did They All Get My Address?](#)
5. [Telemarketing: How to Have a Quiet Evening at Home](#)
6. [Credit Reporting Basics: How Private is My Credit Report?](#)
7. [Workplace Privacy & Employee Monitoring](#)
8. [Introduction to Health & Medical Information Privacy](#)
9. [Wiretapping & Eavesdropping on Telephone Calls](#)
10. [My Social Security Number: How Secure Is It?](#)
11. [From Cradle to Grave: Government Records & Your Privacy](#)
12. [A Checklist of Responsible Information-Handling Practices](#)
13. [Are You Being Stalked?](#)
14. [Privacy When Shopping](#)
15. [Employment Background Checks: A Jobseeker's Guide](#)

Granted, although they do seem to focus more on telecommunications and data security (with virtually nothing on low-profile behavior), what I think is uniquely valuable about PRC's fact sheets is that they concisely give you *many* options of **direct action** that you can undertake *today* without either asking anyone's damn permission or "organizing" a "group" to go do anything, as near as I can tell.

Reformism has *never* solved the grievances of dragnet wiretapping, unjust profiling, or the artificial creation of political prisoners. Security culture, as a strategy for making yourself into a **hard target**, uses a variety of direct action tactics whose efficacy is at least not disproven, given that some methods are proven whereas others are simply unproven (that is, experimental). As the true application of the [precautionary principle](#), security culture blends seamlessly into your life. Regardless of ideology, American political dissidents should begin implementing security culture techniques given their outspoken advocacy of freedom generally; what better way to do so than by practically living it in their own lives as [good role-models](#)?

Postscript: *I'd like to extend a special thank you to [Shane Radliff](#) for all of his assistance in helping me not only prepare my arguments for this series on privacy, but also in organizing all the relevant security culture literature in their entirety. You can listen to [the audio \("spoken discourse"\) version of the entire series](#), as well as [the book reports](#) that inspired me to compile this series in the first place. Finally, be sure to check out all the [freely downloadable security culture literature](#) that was gleaned from a variety of sources.*

Section I:

Telecommunications

A History of Dragnet Wiretapping

 thelastbastille.wordpress.com/2015/03/02/a-history-of-dragnet-wiretapping/

Politicians insist that the government has a “right to know” about the intimate details of an entire citizenry. What they fail to realize is that governments do *not* have rights, which also means that the government has no inherent right to know *anything* about *anybody*. Despite this fundamental truth, these self-imagined rulers arrogantly demand that Americans acquiesce to these invasions of privacy on the grounds of whatever their latest crusade happens to be, yet they insist on maintaining their [state secrets privilege](#). Their desire for the government to become nearly [omniscient](#) is so self-evidently dangerous to liberty that their attempts to implement a [panopticon](#) ought be commonly resisted.

Wiretapping is but just one method of surveillance whose technological and historical antecedent would most likely be the interception of mail. During the American colonial period, the [King’s mandate sanctioned the government’s ability to intercept all mail within the British Empire](#). In post-revolutionary France, [Joseph Fouché](#) intercepted the mails for Napoleon Bonaparte, and [José Rodríguez de Francia](#) intercepted Paraguayan mail throughout the early 19th century. Once the telephone was invented in 1876, it provided yet another way for governments to commit espionage against their own citizens, just like how Nicolae Ceaușescu’s [Securitate](#) combined the techniques of intercepting both mail and telephone communications in Romania.



The Science of Wiretapping

Unlike a sealed envelope, however, the science of the telephone itself does not value individual privacy. Telephones were originally designed to overcome a human limitation, namely, the need to be in the same physical space before talking to someone else during the same moment of time. Once this had been achieved, it was not too long before it was being exploited for a variety of purposes, not only due to its simplistic design, but also because there was little interest in preventing [eavesdropping](#). Wiretapping differs from eavesdropping insofar as wiretapping is one technique of eavesdropping, but not all eavesdropping is wiretapping, as evidenced by putting your ear against a wall or door in order to better listen to the voices on the other side.

Simply put, wiretapping is the act of intercepting telephonic communications; this could be done by installing either [hardwire taps or a transmitting bug within a wall socket, the telephone’s handset, on a nearby telephone pole’s utility junction box](#), a telephone switching station, or the interception of transmissions by other means, such as snatching radio waves out of the air. Whether it be by [landline](#), [cordless](#), [cellular](#), [satellite](#), [ham radio](#), or [VoIP](#), modern telephony is considered private only to the extent that there is a cultural expectation that it should be so, but not so with regards to the inherent nature of the technology itself. What the science of wiretapping appears to tell us is that it is foolish to project one’s false sense of security by crying “foul” after the fact; however, this is not to imply that [technological countermeasures](#) shouldn’t be implemented, for anyone who is serious about his own privacy should move heaven and earth to do so.

The Origins of the National Security Agency

President Harry Truman unilaterally [created the National Security Agency \(NSA\) in 1952](#), specifically for the reason of preventing another Pearl Harbor surprise attack by way of using [signals intelligence \(SIGINT\)](#). In 1976, the [Church Committee](#) hearings revealed that [the NSA had exceeded its foreign intelligence surveillance mandate by monitoring the communications of American citizens](#) whom it deemed were engaging in activities that threatened national security. The committee's [summary of problems](#) included the finding that:

“Governmental officials – including those whose principal duty is to enforce the law – have violated or ignored the law over long periods of time and **have advocated and defended their right to break the law.**” [emphasis added]

Ironically, these illegal abuses by NSA occurred alongside Ceaușescu's Securitate similarly tapping Romanian telephones during the Cold War. Despite another 25 years to get its act together, NSA not only failed to prevent the 9/11 attacks, [but its own internal security was discovered to have been breached a week after the attacks](#). Without missing a beat, the NSA and rest of the [United States intelligence community](#) lobbied Congress to grant them more power as a reward for their infamous failures, and all in the name of national security for this brand new “[War on Terror](#),” whom Brigadier General (now Lieutenant General) [Mark Schissler](#) said [will go on for another 50 – 100 years](#).

Government propagandists will convince people there are dangers that only they can protect us from, but in order to do so, they must first infringe upon our freedoms. From early 20th century organized crime and Cold War communism to modern “[terrorism](#),” civil servants have regularly sought any excuse to increase their power, regardless of who gets hurt in the process, as mere collateral damage. These convenient bogeymen serve their roles well in the quest for inculcating a climate of unjustified fear, which is used by policy makers as a false pretext to make laws hostile to the U.S. Constitution and the American way of life.

The Legality of Wiretapping

Constitutionally, the Fourth Amendment's [Search & Seizure Clause](#) says:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...”

For the sake of political expediency in the wake of 9/11, former President George W. Bush's White House asserted that pursuant to the [Art. II § 2 cl. 1](#) *delegated* power as the Commander-in-Chief of the Army and

the Navy of the United States (and of the Militia of the several States), the [Executive Office of the President](#) enjoyed the *implied* power to wiretap anyone merely suspected of threatening national security. Despite the fact that the Congress has not declared war since World War II (pursuant to [Art. I § 8](#)), the executive branch unilaterally assumed a wartime authority to [run roughshod over the Fourth Amendment](#).

Statutorily, the [Foreign Intelligence Surveillance Act \(FISA\)](#) of 1978 was passed by the Congress into law as the intended political reform in the aftermath of the Church Committee's discovery about the NSA's [Project MINARET](#). FISA created the [Foreign Intelligence Surveillance Court \(FISC\)](#), whose duty it was to determine whether secretive warrants should be issued against suspected foreign spies. The [Communications Assistance for Law Enforcement Act \(CALEA\)](#) of 1994 mandated that telecommunications providers give law enforcement agencies [backdoors](#) for the purpose of easier wiretapping ([eventually for VoIP calls in 2005](#)), and the [Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism \(USA PATRIOT\) Act](#) of 2001 expanded the FISC's **secret** warrants to permit "[roving wiretaps](#)," which [lack the specificity required by the Fourth Amendment](#), and therefore increase the likelihood of incidental intercepts. Ironically, the [FISA Amendments Act](#) of 2008 was passed by the Congress into law as the political reform intended to address the abuses caused by the NSA's [Stellar Wind](#) surveillance program, thereby repeating what had been done exactly three decades previously.

Judicially, the 1928 [Olmstead v. United States](#) case ruled that the Fourth Amendment's Search and Seizure Clause did not apply to the use of wiretaps by federal agents, even if in violation of state law, yet almost 40 years later, [Katz v. United States](#) ruled that the Search & Seizure Clause does protect individuals using a telephone booth from warrantless **eavesdropping**. In his dissenting opinion in *Olmstead*, Judge Louie Brandeis wrote:

*"Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites [anarchy](#). To declare that in the administration of the criminal law the end justifies the means – **to declare that the government may commit crimes in order to secure the conviction of a private criminal** – would bring terrible retribution. Against that pernicious doctrine this court should resolutely set its face."* [emphasis added]

Similarly, Judge William Douglas' concurring opinion in the 1972 [United States v. U.S. District Court](#) (aka, [the Keith case](#)) said:

*"That 'domestic security' is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ **dragnet techniques** to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment."* [emphasis added]

As you could probably tell, the federal judiciary's attitude towards wiretapping (at least before 9/11) wasn't so much about the "reasonableness" of the search and/or seizure in question as it was about the Fourth Amendment's [Warrant Clause](#), which says:

"...and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

In other words, the very lack of specificity *is* unreasonable, [exceptions to the Warrant Clause notwithstanding](#). Supreme Court judges did not want to be perceived as hypocrites, so they devised an interpretative scheme whereby as long as warrants did not emulate a writ of assistance, then it would be appropriate for the courts to try and rationalize the demands of the executive branch against the individual privacy of the average American citizen.

Although this was the United States Supreme Court's rather moderate position before 9/11, the federal district and appellate judiciary's attitude after 9/11 seems quite authoritarian. Judge Lewis Kaplan's 2006 memorandum opinion in [United States v. Tomero, et. al.](#) for the United States District Court for the Southern District of New York ruled that the FBI's installation of [roving wiretap bugs](#) in the defendants' cell phones were not unconstitutional. A year later, Judge Alice Batchelder wrote the United States Court of Appeals for the Sixth Circuit's 2007 decision in [ACLU v. NSA](#), where the plaintiffs lacked standing to challenge the NSA's Stellar Wind surveillance program because they couldn't prove they were directly targeted by it.

The 2011 [Hepting v. AT&T Corp.](#) ruling, written by Judge M. Margaret McKeown on the United States Court of Appeals for the Ninth Circuit, found that legal immunity (against being sued) for the telecommunications companies under § 802 of FISA (which is cross-listed under [Title 50 USC § 1885a](#)) was constitutional. Several months later in 2012, Judge Raymond Fisher conveyed the appellate Ninth Circuit's ruling in [United States v. Olivia](#) that the electronic surveillance orders only authorized "standard interception techniques," and therefore did not convert the defendant's cellular telephone into a roving wiretap bug, despite the fact that the police turned the phone into a roving wiretap. Finally, the [Jewel v. NSA](#) lawsuit (which claimed that [Room 641A](#) inside the SBC Communications building was involved in an NSA dragnet surveillance operation) was dismissed in February of 2015 by Judge Jeffrey White in the United States District Court for the Northern District of California on the grounds that not only could former AT&T technician [Mark Klein](#) not determine "the content, function, or purpose" of Room 641A, but also that the plaintiffs failed to establish "a sufficient factual basis...[that] they have standing to sue under the Fourth Amendment regarding the possible interception of their Internet communications."

Despite the fact that there was no foreign intelligence exception to the Warrant Clause in either the *Tomero* or *Olivia* cases, the federal judiciary frequently use the excuse of statutory construction in order to perform an end run around the Fourth Amendment. This not only contradicts the Keith case, but it also proves both the Church Committee's findings and Judge Brandeis' dissent in *Olmstead* in the ensuing years. [Constitutional avoidance](#), much?

Contemporary Wiretapping

[ECHELON](#) is the code name for some of the SIGINT stations that operate under the auspices of the [Five Eyes intelligence alliance](#), which functions according to the terms of the then [secret treaty](#) known as the [UKUSA Agreement](#). Right off the bat, there is a question of constitutionality here, for the Advice & Consent Clause ([Art. II § 2 cl. 2](#)) says, in part:

“He [the President] shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two-thirds of the Senators present concur...”

There is no public record available testifying to the fact that the U.S. Senate ever ratified any treaty with either England, Canada, Australia, or New Zealand, since the end of the Second World War, to openly share signals intelligence. Not only that, but it wasn't until July of 2001 when the [European Union Parliament issued a report](#) confirming the existence of ECHELON, the UKUSA Agreement, and the Five Eyes SIGINT network.

What is truly disconcerting, though, is that as the foundational basis for the UKUSA Agreement, the NSA works around statutory limitations, like FISA, by having either the [Communications Security Establishment](#), the [Government Communications Headquarters](#), the [Australian Signals Directorate](#), or the [Government Communications Security Bureau](#) collect SIGINT from Americans, who then turn around and hand it to the NSA for whatever “national security” purposes they see fit to exercise, such as building the [Utah Data Center](#) in order to store [massive amounts of information](#).

For all intents and purposes, the UKUSA Agreement has permitted these four other governments to commit espionage against Americans, and then share that information with the NSA, thereby circumventing the Constitution.

Relying on a combination of transatlantic underwater cables and orbital geostationary satellite uplinks and downlinks, ECHELON provided the framework necessary to implement a plethora of wiretapping tools. For instance, both [PRISM](#) and [MUSCULAR](#) collect not only metadata, but also the content of VoIP calls. Whether or not [black rooms](#) like Room 641A or the roving wiretap bugs have anything to do with the NSA is anyone's guess, but what all of them demonstrate is that the federal government does not care about your individual privacy, and even less so about the rule of law.

Take, for instance, how the federal government treats NSA whistleblowers. [Perry Fellwock](#), [Russell Tice](#), [Thomas Tamm](#), [William Binney](#), [Thomas Drake](#), and [Ed Snowden](#) have all been persecuted by the United States government. Costly litigation, pension revocations, and seeking political asylum as a fugitive are but just some of the consequences experienced by these whistleblowers, who under pain of individual conscience, chose to reveal the abuses perpetrated by the NSA. Accusations that these whistleblowers are so-called “[limited hangouts](#)” ought to be placed under scrutiny for ulterior motives.

Let us now review this history of dragnet wiretapping. The sequence of events are as follows:

- 1760s – 1770s: colonial mail intercepted by Redcoats
- 1799 – 1814: Joseph Fouché intercepted French mail for Napoleon Bonaparte
- 1814 – 1840: José Rodríguez de Francia intercepted Paraguayan mail

- 1876: the invention of the telephone
- 1928: *Olmstead v. United States*, 277 US 438
- 1952: President Truman's memo creating NSA
- 1955: [updated UKUSA Agreement](#)
- 1965: Nicolae Ceaușescu began interception of Romanian mail & wiretapping
- 1967: *Katz v. United States*, 389 US 347
- 1968: [Omnibus Crime Control and Safe Streets Act](#) (aka, the "Wiretap Statute")
- 1972: *United States v. U.S. District Court*, 407 US 297
- 1976: Church Committee hearings
- 1978: Foreign Intelligence Surveillance Act (FISA)
- 1988: [Electronic Communications Privacy Act](#) (ECPA)
- 1989: Ceaușescu executed by firing squad; mail interception & wiretapping ended
- 1994: Communications Assistance for Law Enforcement Act (CALEA)
- 1998: Hollywood film [Enemy of the State](#) released into theaters
- 2001, July: EU Parliament report on ECHELON
- 2001, October: USA PATRIOT Act
- 2004: [A False Sense of Insecurity?](#) article
 - A libertarian analyst evaluated the true risk of "terrorism"
- 2005: [Stellar Wind publicly revealed](#)
- 2006: *United States v. Tomero*, S2 06 Crim. 0008
- 2007: *ACLU v. NSA*, Nos. 06-2095/2140
- 2008: FISA Amendments Act
- 2011: *Hepting v. AT&T Corp.*, No. 09-16676
- 2012: *United States v. Olivia*, No. 10-30126
- 2013: [Liberty & Security in a Changing World](#) report
 - The Obama White House's official story after Ed Snowden's leaks
- 2015: *Jewel v. NSA*, No. 08-04373

This chronology demonstrates that the interception of communications, and wiretapping specifically, is nothing new. Whether it is by way of legislation or court precedent, the American federal government absolutely refuses to be bound within the chains imposed upon it by the U.S. Constitution. No amount of [reformism](#) will reign in the persistent abuses by the NSA. What it can't take by a large bite, they will take by smaller bites. Nothing less than total abolishment of this nefarious [administrative agency](#) would even begin to satisfy the demands of natural justice.

Counter-Wiretapping Remedies

Fortunately, the [cypherpunks](#) and [crypto-anarchists](#) are here to help Americans fend off the NSA in the

ongoing [crypto wars](#). An eclectic mixture of [free and open-source software](#), [public-key cryptography](#), and [end-to-end encryption](#) can be used to supply the market demand for inexpensively available [secure telephones](#), whose development should not be as elusive as that of cold fusion. Since encryption is like a sealed envelope, nearly all popular voice communications might as well be verbal postcards. If [the OpenPGP standard is already used to encrypt email](#), and [OTR is similarly being used to encrypt instant messages](#), then there is no good reason that I can fathom as to why [ZRTP](#) (Zimmerman Real-time Transport Protocol), or similar software, cannot be built to encrypt at least VoIP, if not also cellular, calls. We need to use secure communications, if we're going to have a reasonable expectation of privacy. This becomes particularly critical for [security teams](#), [local Committees of Safety](#), and any other communications that you feel that the government should not have access to.

With every failure, government is rewarded with more power. From Pearl Harbor to the [Boston Marathon bombing](#), the NSA is not only a catastrophic [lead balloon](#), but also the ears of, what some might call, the slowly emerging [New World Order](#). Because of [dragnet wiretapping's inherent threat to individual privacy](#) is why the adage, "Don't say anything on the phone you wouldn't also be comfortable repeating in front of a cop, a judge, or a jury," carries so much sway. [As Eric Hughes wrote back in 1993](#):

"Privacy is the power to selectively reveal oneself to the world...[t]o encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy...[w]e must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do."

Free market technology, not government law, is the solution. Do we want to resort to "whispers, darkness, envelopes, closed doors, secret handshakes, and couriers," or do we want to pursue modern techniques for the maintenance of our right to privacy, as enumerated by the Fourth Amendment, as the Framers intended? About 87 years have passed since the *Olmstead* ruling, and I'll be damned if another decade goes by without me pulling my weight for the cause of liberty. And now that you have read this history of wiretapping, you must ask yourself, [are you interested?](#)

Data-mining the Haystack: Should You Attempt to Overload the NSA's Servers with “Suspicious” Email Keywords?

□ www.thelastbastille.com/2016/02/18/data-mining-the-haystack-should-you-attempt-to-overload-the-nsas-servers-with-suspicious-email-keywords/

*“The problem was not that we weren’t collecting information, it wasn’t that we didn’t have enough dots, it wasn’t that we didn’t have a haystack – it was that we did not understand the haystack that we have. The problem with mass surveillance is that we’re piling more hay on a haystack we already don’t understand. And this is the haystack of the human lives of every American citizen in our country. If these programs aren’t keeping us safe, they making us miss connections, **vital** connections, on information we already have, if we’re taking resources away from traditional methods of investigation, from law enforcement operations that we know work, if we’re missing things, like the Boston Marathon bombings, where all of these mass surveillance systems, where every domestic dragnet in the world didn’t reveal guys that the Russian intelligence service told us about **by name**, is that really the best way to protect our country? Or are we trying to throw money at a magic ‘solution’ that’s not just costing us our safety, but our rights and our way of life?”*

– Edward Snowden



Misinformation abounds when it comes to mass [data-mining](#). Typically, the federal government will either deflect attention by stressing they are collecting **only** foreign intelligence (*not* domestic intelligence) or that they are **only** collecting metadata (*not* the content of your communications). Whether it be by way of the [USA PATRIOT Act's § 215](#) or [FISA's § 702](#), the fact of the matter is that any hypothetical “limits” imposed by these statutory laws don’t matter, and [the constitutionality of them even less so](#), considering [the history of the unconstitutional National Security Agency \(NSA\)](#).

All of these excuses for **strictly** foreign and/or metadata intelligence gathering by the NSA is really quite spurious for two major reasons – ECHELON and the [Utah Data Center](#). Back in July of 2001, the [European Union Parliament issued a report](#) that admitted to the existence of ECHELON as a signals intelligence (SIGINT) network of the [Five](#)

Eyes intelligence alliance, which was established by the [UK-USA Agreement](#). The Utah Data Center was exposed a few years ago as being part of both STELLAR WIND as well as the Department of Defense's [Global Information Grid](#), which handles data to the magnitude of [yottabytes](#) (that's equivalent to 1 trillion [terabytes](#)). Between ECHELON and the Utah Data Center, the NSA has no *practical* or *technical* reason to "limit" its own power, given that the NSA collects **domestic** intelligence (including **content**) through their foreign allies who spy on Americans, and then they store all that information in approximately \$2 billion worth of cloud computing.

Despite all this, there is still a naïve belief in the virtues of [reformism](#). It matters not that the [FISA Amendments Act](#) ("the reform of the reform," as it were) *expanded* the scope and authority of § 702, but rather the fact that surveillance programs like [PRISM](#), [MUSCULAR](#), and [XKeyscore](#) were only possible because each one of them were an *expansion* upon the Five Eyes' ECHELON system, which itself exploits the [Internet's backbone](#). What I inferred from a few [declassified FISC rulings from over two years ago](#) was that this whole "bundling" claim is disingenuous too, because if the NSA knew from a purely technical standpoint that indiscriminate data-mining was unavoidable, then they shouldn't be doing it *at all*, simply due to the fact that such bulk data collection is *at least* a search, if not also a seizure, of one's "papers and effects" through the Internet, and is therefore a blatant violation of the Fourth Amendment. No amount of "reforming" the NSA is even applicable to [GCHQ](#), [CSE](#), [ASD](#), or [GCSB](#) in the first place, especially in terms of curbing their espionage against the communications of the American citizenry.

Taking this as a given, the NSA has got to put all that SIGINT they got from their foreign allies, *somewhere*, right? William Binney, a NSA whistleblower, warned that the Utah Data Center engaged in [deep packet inspection](#) of email, specifically. This distinction made by government apologists between foreign versus domestic spying is largely irrelevant, not only because of the Five Eyes network, but also the fact that many email servers are themselves located offshore, and therefore susceptible to SIGINT espionage by the NSA. The reason the Utah Data Center is geared towards storing yottabytes worth of information is simply because that very intelligence is not just metadata, but content as well; otherwise, they wouldn't need that kind of storage space now, would they?

Remember, the federal government still insists on exercising its "[states secrets privilege](#)" as a matter of **public policy**, so you have to ask yourselves – do you honestly think that *any* high-level government official would be willing to brazenly lie to the public if by doing so he would be preserving classified "national security" procedures? [Congresscritter Hank Johnson questioned then-NSA chief General Keith Alexander](#) about the NSA's technical capability in intercepting SIGINT during a congressional subcommittee hearing on March 20th of 2012 (*before the Snowden leaks*); the [general flat out denied in his testimony](#) that the NSA collected bulk data of Americans' communications, including content. Consider also these statements made by Barack Obama back on July 7th of 2013 (post-Snowden), where he did admit that the NSA collected metadata on American citizens:

"Nobody is listening to your telephone calls."

"Now, with respect to the Internet and emails, it does not apply to U.S. citizens and it does not apply to people living in the United States..."

"They do not involve listening to people's phone calls, do not involve reading the emails of U.S. citizens or U.S. residents."

Now, if all of this email and phone surveillance is unquestionably and completely legal, then would *el presidente* please be kind enough to explain to everyone why there are as many credible NSA whistleblowers as there are? Is the Tyrant-in-Chief implying that they all just exaggerated a bit too much, and therefore *deserved* all of the

harassment and sometimes outright persecution they faced? Or is there serious foul play afoot?

Decades ago, [William Knowles](#) suggested that it might be worth “overloading” the NSA’s servers with “suspicious” keywords. Fast-forward to 2013 when **Vice** attempted to do just that with its [Hello, NSA](#) random keyword laced message generator; yet, this was more of an attempt to [hamper the ability of the NSA to data-mine “social media” websites for open-source intelligence](#), as evidenced by [DHS’ redacted 2011 Analyst’s Desktop Binder](#). Concurrently, there was a similar attempt to obfuscate the value of any bulk data collection, as well as call the President’s bluff that the NSA does not listen to phone calls or read emails, by [Operation Troll the NSA](#), which encouraged the public to call and/or email a script containing these “suspicious” keywords on the same day. Naturally, as is typical with all “critical mass” protests, there was no measurement metric taken by which to gauge the effectiveness of such a (presumably) widespread action.

Let’s talk shop, shall we? [The average email size is roughly 75 kilobytes](#), without attachments. If we make an assumption that the Utah Data Center has a maximum storage capacity of a single yottabyte and divide that by the average email size, then it would take 40 quintillion emails to fill it (given that one yottabyte equals one sextillion kilobytes). Since the total American population is estimated to be 323 million people, and assuming that each one of them sent out 100 emails a day without fail, then it would take them 80 billion years to reach the Utah Data Center’s presumed maximum capacity.

I think you can tell by the results of my calculations that the average email is the smallest conceivable file size, whereas the Utah Data Center is the largest conceivable set of cloud computing servers; therefore, this presumption that nearly innumerable swarms of keyword laden emails could ever make the slightest of dents into overwhelming the NSA’s servers is pure foolishness. If you were to attempt such a dent, it would’ve been better to use the largest conceivable file size that has the highest possibility of successful file transferal without interruption or glitches, such as [those videos that feature 10 hours of elevator music](#). Obviously, this would be something akin to the [black fax](#) method, which attempts to run the black ink within printers dry through sheer waste.

It is more than fair to say that the efficacy of email keywords “overloading” the NSA’s servers has not been proven; what evidence and arguments have been presented here are a critique that is offered in good faith. Advocates of this method bear the burden of proof for demonstrating its efficacy, not me or any other critics. Suffice it to say, I don’t think those proponents have met their burden of proof, and what evidence is available suggests that their purported method is unfeasible, especially considering the obvious failure that was Operation Troll the NSA. What is the solution here, then, if not “overloading” the NSA’s servers with “suspicious” email keywords?

The solution is, therefore, *not* using keywords to either “trip” or “overload” anything, but rather encryption. In this case, since the concern is about emails being data-mined and read by intelligence analysts, the specific encryption type would be [Pretty Good Privacy](#) (PGP). Nearly two years ago, I wrote two different tutorials for configuring PGP with your operating system; [one for a Windows OS](#), and [another for a Mac OS](#). Within [the EU Parliament’s 2001 report about ECHELON](#), they recommended the use of encrypted email:

“In contrast [to telephones], e-mails can and should be encrypted by everyone. The oft-repeated claim that a person has no secrets and thus has no need to encrypt messages must be countered by pointing out that written messages are not normally sent on postcards. However, an unencrypted e-mail is nothing other than a letter without an envelope. The encryption of e-mails is secure and relatively straightforward and user-friendly systems, such as PGP/GnuPG, are already available, even free of charge, to private individuals on the Internet. Unfortunately, they are not yet sufficiently widely distributed. The public authorities should set a good example and themselves employ encryption as a standard practice in order to demystify the process.”

Now, [GNuPG](#) is sufficiently widely distributed, and considering the prevalence of crypto-currencies like [Bitcoin](#), any excuses of computer illiteracy simply get tossed out of the window for the rubbish that it is. As long as you have electricity and Internet access, you can use PGP encrypted emails, once it's been configured.

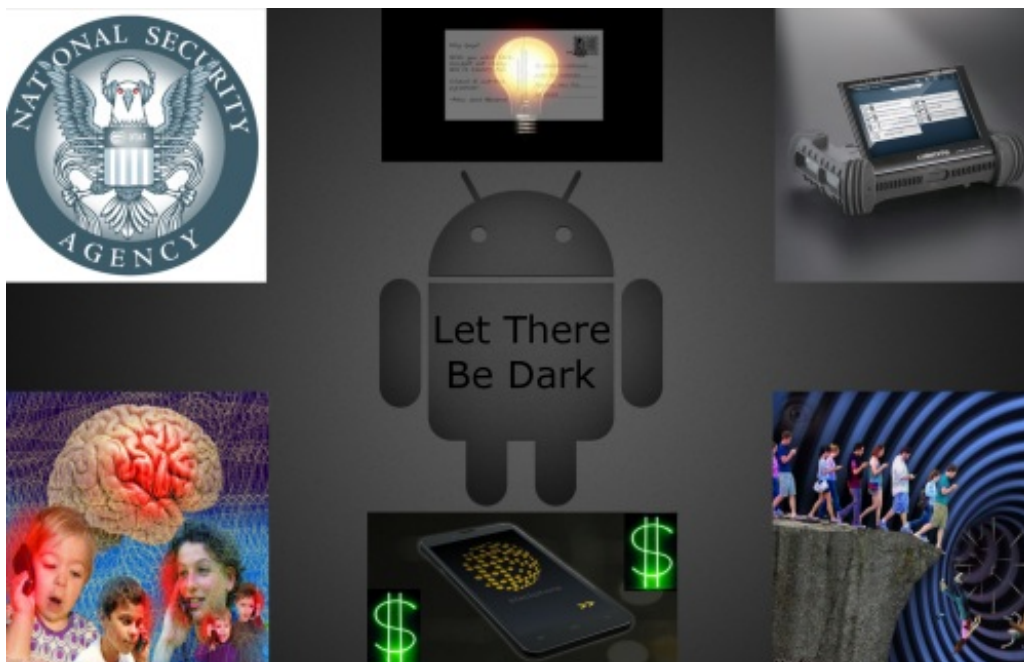
Since the NSA is indiscriminately data-mining nearly everyone, I'm sure they've got a copy of [Hillary Clinton's missing Benghazi emails](#), am I right? Either way, the more serious issue is that too many American dissidents of various ideologies are, oddly enough, stubbornly consistent in their practice of making all manner of excuses in order to *not* practice good [security culture](#). If they took one-tenth of that effort in *avoiding* the practice of security culture techniques and redirected it towards learning these methods, then they'd already be using them well enough for it to be beneficial to them. Why there is this tendency to needlessly increase one's opportunity costs is a mystery I intend to solve, for it would explain their aversion towards what does work, as well as their attraction for what does not work, in terms of helping them secure their own personal liberty.

Are Cellular Telephones Furthering Human Liberty?

www.thelastbastille.com/2016/06/06/cellular-telephones-furthering-human-liberty/

"Can you remember a time when you went for a walk or out to the shops or even commuted home to and from your job without the need to carry around a mobile phone? Today's phones feature GPS tracking, wireless network hookup and even allow Google the knowledge of your exact physical location for improved search and 'other services.' We have sold the freedom of privacy, friends, and in attempting to avoid ever being alone again we have isolated ourselves by becoming enslaved to our gadgets...[s]o here we are, suckered into thinking we are in communication with others at all times, yet limiting ourselves in actual ability to communicate clearly by crippling the English language in order to save time on sending text messages. Save time for what? More World of Warcraft?"

– [The Anti-Terrorist](#)



Introduction

Technology is a double-edged sword. It can be used for good ends, but it also be used to commit unspeakable evil. Whether it is used for one or the other ultimately depends on the choices that are made by individuals. Understanding how any technology works is pivotal in exercising free will by way of making informed choices.

Shane Radliff has recently discovered that it is indeed possible to browse the Internet and [talk anonymously using cellular telephones](#). This is chiefly accomplished through buying prepaid mobile phones, activating them using as little personally identifiable information (PII) as possible, and then configuring them with smartphone apps that encrypt both text and voice communications using digital encryption protocols like [Off-the-Record](#) (OTR) and the [Zimmerman Real-Time Protocol](#) (ZRTP). Developments in the on-going crypto wars will reveal over time whether free and open-source software, as used by the people, have an indispensable role in preventing the deciphering of digitally encrypted material by the government's cryptanalysts.

Personally, I think the more fundamental question revolves around whether cell phones are mostly beneficial or

noticeably detrimental to individual liberty. [Security culture](#) is only valuable to the extent that its practitioners are less vulnerable to coercion than those who fail to take their right to privacy seriously. Weighing both the pros and cons of cell phone ownership necessarily entails a thorough grounding as to how such an invention has a multi-faceted significance within your own life.

Search Warrants, Fourth Amendment “Papers,” & Color of Law

Any constitutionalist worth their salt knows that the [Fourth Amendment’s Warrant and Search & Seizure Clauses](#) are the legal protections against indiscriminate surveillance, including [dragnet wiretapping](#). While the right to privacy is not enumerated like the [right to keep and bear arms](#) or the [right of peaceful assembly](#), the constitutional limits upon searches, seizures, and the issuance of warrants did inadvertently value individual privacy. Unfortunately, the federal judiciary’s constitutional interpretations of the Fourth Amendment are typically weighed against the citizenry, especially when cellular telephones are at play.

In 2006, Judge Lewis Kaplan’s memorandum opinion in [United States v. Tomero, et. al.](#), under the auspices of the United States District Court for the Southern District of New York, ruled that the FBI’s installation of roving wiretap bugs in the defendants’ cell phones were not unconstitutional. Six years later, Judge Richard Posner wrote the United States Court of Appeals for the Seventh Circuit’s decision in [United States v. Abel Flores-Lopez](#) that a warrantless search of the defendant’s cell phone in order to verify the cell phone’s number was not a violation of the Fourth Amendment. Five months later in 2012, Judge Raymond Fisher conveyed the federal appellate’s Ninth Circuit decision in [United States v. Ortiz Oliva](#) that the electronic surveillance orders only authorized “standard interception techniques,” and therefore did not convert the defendant’s cell phone into a roving wiretap, despite the self-evident fact that the police, indeed, turned the phone into a roving wiretap.

About a month later in August of 2012, Judge John Rogers delivered the opinion of the U.S. Court of Appeals for the Sixth Circuit in [United States v. Melvin Skinner](#), which ruled that the defendant’s lack of knowledge about his cell phone’s [geolocation](#) capabilities did not give him an expectation of privacy, especially against police surveillance. In both [May](#) and [August of 2013](#), the United States District Court for the District of Arizona’s Judge David Campbell repeatedly decided that the [2008 Tracking Warrant](#) for the defendant’s cell phone did not violate the Fourth Amendment since the aircard was bought by way of identity theft, according to these court documents from the [United States v. Daniel Rigmaiden](#) case. On January 11th of 2016, the [United States Supreme Court denied a petition for a writ of certiorari](#) in the [EPIC v. DHS](#) case, which was all about whether or not the federal government possessed an Internet kill switch that would also simultaneously shut down cellular towers during the onset of a government declared emergency.

Whether the specific issues of these half dozen federal court cases dealt with roving wiretap bugs, geolocation, kill switches, defective warrants, or warrantless searches of the cell phones themselves, these federal judges consistently ruled against the defendants’ right to privacy, largely on the presumption that accused criminals have no expectation of privacy, even if they were engaging in “criminally victimless” activity. The bugging of a defense lawyer’s cell phone in the 2006 *Tomero* case is particularly troubling, for Judge Kaplan explained that:

“By February 2004, the government had learned that Peter Peluso, an attorney and close associate of Ardito, was relaying messages to and from high-ranking family members who were wary of government listening devices and who used Peluso as a messenger to avoid meeting together directly. In a renewal application dated February 6, 2004, the government sought, and Judge Jones in due course granted, authority to install a roving bug in Peluso’s cellular telephone. This order was renewed several times throughout 2004, as the government continued to identify locations where

Peluso and Ardito discussed family matters and learned that the subjects were growing increasingly cautious of government surveillance.

"In January 2005, Peluso agreed to cooperate with the government's investigation. At that point the government removed the listening device in his cellular telephone and Peluso began recording conversations with family members consensually by wearing a microphone. On July 7, 2005, Peluso pleaded guilty, pursuant to a cooperation agreement with the government, to a four-count information, charging him with, among other things, engaging in a pattern of racketeering activity."

So, much for [attorney-client privilege](#), huh? Notice also that Peluso turned state's evidence 11 months after the roving bug was placed, most likely after the government police Bluecoats informed him of what they had on him in terms of criminal charges and the harshness of the maximum sentence. Just as soon as Peluso had betrayed his clients, only then was the roving bug in his cell phone removed to then be replaced by a wire that he wore on his person.

I guess that if an investigative journalist was working a story and then accused by the government for anything, then the only way he could still work on the story would be to become an indentured serf for the prosecutor; whether the "professional" under the thumb of the government be an attorney or a journalist, you would think a possible legal defense against this practice would be for the defendant's counsel to issue a [Fifth Amendment self-incrimination](#) challenge, but unfortunately, such was not argued here in the *Tomero* case. In the 2012 *Flores-Lopez* case, Judge Posner wrote:

*"In some cases, a search of a cell phone, though not authorized by a warrant, is justified by police officers' reasonable concerns for their safety. One can buy a stun gun that looks like a cell phone... [b]ut the defendant's cell phone, once securely in the hands of the arresting officer, endangered no one. It did, however, contain evidence or leads to evidence – as the officers knew was likely because they knew from their informant that as is typical of drug dealers the defendant had used cell phones to talk to Santana-Cabrera and other coconspirators. But was there any **urgency** about searching the cell phone for its phone number? Yet even if there wasn't, that bit of information might be so trivial that its seizure would not infringe the Fourth Amendment."*

What kind of pabulum is this? Apparently, the cult of "officer safety" still had ardent believers who impose their faith within secular courtrooms. Judge Posner continually draws on previous court case precedent:

"So, opening a diary found on the suspect whom the police have arrested, to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested, clearly is permissible; and what happened in this case was similar but even less intrusive, since a cell phone's phone number can be found without searching the phone's contents, unless the phone is password-protected – and some cell phones even if it is...[i]t's not even clear that we need a rule of law specific to cell phones or other computers. If police are entitled to open a

pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number."

Last time I checked, the Fourth Amendment applied to the people's "persons, houses, papers, and effects." **If a diary does not count as one's "papers," then what does?** Judge Posner finally concluded that a cost-benefit analysis by the police Bluecoats would not be feasible to do prior to searching a suspect under arrest. According to the 2012 *Oliva* ruling, Judge Fisher said:

"The 'off the hook' language, however, lacks meaning when applied to cellular phones. Terminating a call on a cellular phone does not turn the phone completely off. To do so requires a separate and more deliberate step that the user may not appreciate is necessary, and may leave the cellular phone open to electronic eavesdropping quite different from what can occur with accidentally failing to hang up a land line phone. Unlike a relatively stationary land line phone, a cellular phone whose microphone remains on even though the call is terminated becomes a truly 'roving bug.' If that is what the government's application for a warrant actually seeks, it cannot do so using arcane, outmoded terminology like 'off the hook.'"

Whether we're talking about roving bugs or roving wiretaps (pursuant to the [Omnibus Crime Control & Safe Streets Act of 1968](#)), the fact of the matter is that *Oliva's* motion to suppress the evidence collected under the guise of a dubious warrant was denied. Judge Rogers, in the 2012 *Skinner* case, wrote:

"There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone. If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this. If it did, then technology would help criminals but not the police. It follows that Skinner had no expectation of privacy in the context of this case, just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car's paint."

It would seem to be the case that Judge Rogers thinks that technological ignorance (or even illiteracy) does not justify the defendant's expectation of privacy, because he equated the cell phone's GPS signaling to tracking hounds and getaway cars as the mere tools of both the police and the "criminals" they apprehend, respectively. Interestingly enough, this concept was explained more in depth by Judge Campbell in the 2013 *Rigmaiden* case; [according to](#)

the May 8th court order:

“One who so thoroughly immerses himself in layers of false identities should not later be heard to argue that society must recognize as legitimate his expectation of privacy in the location and implements of his fraud...[d]efendant did not have an expectation of privacy society is willing to accept as legitimate.”

So, the tools used by defendants and the government are fair game, unless the defendant is being accused by the prosecutor of acquiring those tools through fraud. Either way, the **defendants have no expectation of privacy**, regardless of whether they “voluntarily procured” their own tools, or acquired them fraudulently. In other words, if the government charges you with a crime, then your right to privacy will be infringed upon.

Underlying all of this jurisprudence is the [color of law](#) being committed by these judges, as well as the inevitable consequence that is the [fruit of the poisonous tree](#). The origin of this seems to be a case that was frequently cited in *Tomero*, which was the 1993 [United States v. L. Bianco](#) case that was decided by the federal Court of Appeals for the Second Circuit. Judge George Pratt wrote for the appellate panel (referring to a home that was used to conduct a ritualistic ceremony), saying:

“Since none of the defendants had any legitimate interest in the privacy of the 34 Guild Street residence before they arrived there, they lack standing to assert that the entry to install listening devices inured their rights.”

Now, by examining some references in *Tomero*, I think the “fruit” of legitimizing the roving bugs & roving wiretaps becomes rather apparent:

*“Defendants point first to the fact that the order in **Bianco** authorized the placement of listening devices only in buildings whereas the order here authorized placement in mobile telephones. But the argument misses the point.*

*“The essence of the motion to suppress is that the statute unconstitutionally permits interception in the absence of any specification of the place where communications are to be intercepted. In **Bianco**, the Second Circuit rejected precisely this argument. The fact that the unspecified location in **Bianco** happened to be in a building had nothing to do with the holding. Furthermore, while a mobile device makes interception easier and less costly to accomplish than a stationary one, this does not mean that it implicates new or different privacy concerns. It simply dispenses with the need for repeated installations and surreptitious entries into buildings. It does not invade zones of privacy that the government could not reach by more conventional means.”*

Well, there's your [common law](#) for you. The *Tomero* defendants' as-applied challenge was rejected by the court, even though there is a substantive difference between wiretapping a cell phone and bugging a room, as the later was the case in *Bianco*; this set the stage for the successful prosecution of the *Oliva* defendants, because the precedent had already been laid by *Bianco* and *Tomero*.

Something not too dissimilar could be said about warrantless searches and geolocation. The color of law here would seem to begin with *Flores-Lopez*, "just" for the purpose of warrantlessly "validating" the defendant's cell number, which would be considered metadata. Later in *Skinner*, actively tracking the cell phone remotely was warrantlessly permissible because the defendant wasn't careful enough in disabling the geolocation feature. This set the stage for *Rigmaiden*, where the fruit of the poisonous tree ripens, which is all thanks to Judge Campbell's interpretation that the warrant was valid because the defendant was suspected of using his fraudulently acquired tools to commit more crimes (this would be comparable to a presumption that if you did not have your return address on a letter, then the Bluecoats could just assume nefarious activity and then proceed to open your mail). The similarity between *Flores-Lopez*, *Skinner*, & *Rigmaiden* is that although there was no wiretapping as in the other trio of aforementioned cases, the remote tracking as well as the physical search & seizure of the cell phones in question was tipped heavily in favor of the prosecutor, based on the assumption that the mere "suspicion" of "criminal" activity "suspends" the defendant's right to privacy, and by extension, due process as well.

What are the implications of all this judicial precedent? It would appear to be the case that the issuance of what historically would be considered to be general warrants (more specifically, the historical writs of assistance opposed by the American colonists) have already found themselves a comfortable home on the benches of the federal judiciary. Since a few of the previously mentioned judges easily dismissed the particularity requirement of the Fourth Amendment's [Warrant Clause](#), especially with regard to the roving intercepts of both wiretaps and bugs, then it seems to me that Judge Louie Brandeis' warning in his dissenting opinion of the 1928 *Olmstead v. United States* case has been validated once again, but this time it had nothing to do with national security or "terrorism" issues at all.

Fundamentally, I think the question at law to be answered is this – **are the contents of a cell phone equivalent to the "papers" enumerated in the Fourth Amendment?** Remember, the sequence of events matter; would anyone tolerate a Bluecoat rummaging through your drawers at home and seizing your papers *without* a warrant, simply because he testified on the witness stand later that he was concerned you might burn them before he arrived at your home? If not, then wouldn't flushing illicit narcotics down the toilet *before* a police raid fail to count as "destruction of evidence?"

Put another way, would wiping your cell phone *prior* to the issuance of a warrant be equivalent to burning your papers *before* the police are breaking down your door? If not, then why would it be considered "destruction of evidence" *prior* to the issuance of a warrant? Government prosecutors love it when statutory provisions are construed as broadly as possible by the judges for their witch-hunts, but absolutely hate it when defendants attempt to do the exact same thing in defense of their rights.

Truth be told, what these half dozen cases reveal is a profound lack of legal protections for cell phone users, regardless of the issues at law or the subject matter the facts of the case revolve around. The fact of the matter is that cell phone users are legally quite vulnerable to both data-mining and wiretapping by the police, and it should be clear by now that different types of Fourth Amendment challenges have already been tried and failed miserably. Unless someone litigates a test case by getting a federal judge to legally rule on determining what counts as Fourth Amendment "papers," then I don't foresee any other legal defenses against the federal judiciary using color of law to plant the seed for the fruit of the poisonous tree.

Digital Encryption's Trustworthy Security?

Believe it or not, the 1968 Wiretap Statute did not only authorize roving intercepts, but also the issuance of annual wiretap reports to the United States Congress. According to the [2012 Wiretap Report](#), total wiretaps were reported to be 3,395; in 2013, there were 3,576 total wiretaps, and 3,554 total wiretaps were reported for 2014. Interestingly enough, these latest three Wiretap Reports also had something to say about the increased use of encryption, respectively:

"Encryption was reported for 15 wiretaps in 2012 and for 7 wiretaps conducted during previous years. In four of these wiretaps, officials were unable to decipher the plain text of the messages. This is the first time that jurisdictions have reported that encryption prevented officials from obtaining the plain text of the communications since the AO [Administrative Office] began collecting encryption data in 2001."

"The number of state wiretaps in which encryption was encountered increased from 15 in 2012 to 41 in 2013. In nine of these wiretaps, officials were unable to decipher the plain text of the messages. Encryption was also reported for 52 state wiretaps that were conducted during previous years, but reported to the AO for the first time in 2013. Officials were able to decipher the plain text in all 52 intercepts."

"The number of state wiretaps in which encryption was encountered decreased from 41 in 2013 to 22 in 2014. In two of these wiretaps, officials were unable to decipher the plain text of the messages. Three federal wiretaps were reported as being encrypted in 2014, of which two could not be decrypted. Encryption was also reported for five federal wiretaps that were conducted during previous years, but reported to the AO for the first time in 2014. Officials were able to decipher the plain text of the communications in four of the five intercepts."

Consider for a moment the implications of these findings. Although they admitted a specified number of encrypted wiretaps that they were unable to decipher, if you were to calculate the number of encrypted wiretaps they *were able* to decipher, I think you will find very quickly that they were able to decipher the **majority** of the encrypted wiretaps. If accurate, then that would mean that they can crack quite a bit of encryption, just not all of it, for some reason.

One likely reason this is the case, I speculate, is because different cell phone apps use different protocols. [Shane Radliff engaged in consumer testing of various assorted cell phone digital encryption apps on his iPhone three months ago](#), yet while he seemed positive about his experience using those apps, he did point out that Surespot was mentioned in the *United States v. Ali Shukri Amin* case. According to the [Statement of Facts](#), it says:

"On January 16, 2015, an overseas ISIL supporter communicated to the defendant via Surespot that the group of ISIL supporters, including RN, had successfully crossed over into Syria."

Think about that for a moment – how would the prosecutor and defense counsel *both know* that a terrorist had

contacted Amin using Surespot? Unless someone [snitched](#), the only other possibility I can fathom is that the call was intercepted by the National Security Agency and cracked; given the metadata would show that it was an overseas call, it's not unreasonable conjecture to say that the NSA hacked Surespot's encryption and discovered the nature of the communication between Amin and his associate.

What about the late [FBI-Apple encryption dispute](#)? It's been seldom reported in the mainstream media that FBI Director James Comey admitted that [the Bureau paid over \\$1,300,000 to grey hat hackers to crack the San Bernardino shooter's iPhone](#). Once that was done, the (in)Justice Department withdrew its litigation against Apple that had attempted to coerce them into developing either a backdoor or a virus that would enable the Bureau to access the shooter's cell phone. [According to Comey](#), the one-time hack only works on the iPhone 5C, but not the 6S or even 5S.

Does the FBI's outsourced hack of Apple's encryption really even matter? Back in 2009, Apple persecuted its own users for [jailbreaking](#) their own iPhones, because they alleged that doing so infringed on their copyright; it wasn't until 2010 when [the Librarian of Congress made the decision](#) to allow exemptions to what was otherwise the prohibitions on the circumvention of copyright protection systems (like digital rights management). Given that [Ed Snowden whistle-blew Apple's involvement with PRISM](#) only three years ago, I doubt Apple really gives a damn about users' privacy, which is why Mac users like myself have been gradually using more [free and open-source software](#) while lessening dependency on their proprietary software.

WTHR, an Indianapolis NBC affiliate, reported in 2008 [about the prevalence of cell phone spyware](#), which had the capability to wiretap calls and geolocate the phone itself. Eight months later in 2009, WTHR's followup report featured a digital security firm that pioneered the capability to [remotely backup and then wipe a cell phone using GPS tracking](#). This company's chief technology officer also said that they had developed software capable of detecting and removing spyware and viruses.

Although that might be comforting and rather forward thinking of them at the time, an Israeli firm known as [Cellebrite](#) developed technology exclusively for the "law" enforcement Bluecoats. Specifically, their UFED devices are used to perform computer forensics on cell phones, such as memory dumps, cross-referenced data analysis, and most alarmingly, defeating both user locks and encryption protocols. As one of Cellebrite's [company pamphlets](#) brags:

*"As the sheer number of mobile numbers grows, so too does the volume and complexity of data they contain. Having the right mobile forensic tools at the ready to extract that data quickly has never been more important. The UFED Series delivers the most comprehensive mobile forensics extraction and decoding capabilities on the market. Flexible and secure, our unique solution makes it easy for forensic specialists to access and import mobile, location, private cloud and operator data from the widest range of mobile and GPS devices. With it, **officers, investigators and lab examiners can quickly and effectively bypass device user locks, decrypt encrypted data from rapidly changing device operating systems and recover texts, deleted emails, location information and account profile data** – and take appropriate action." [emphasis added]*

If a police officer like the one in the 2012 *Flores-Lopez* case had a UFED device, then the sky would've been the limit as to what other potential charges the prosecutor could have alleged. However, if UFED's [data extraction](#) technology has been around for several years, then it begs the question as to why the FBI didn't use their technology during the public relations controversy with Apple? Perhaps it had something to do with Fox News correspondent [Carl Cameron](#)'s four-part exposé on [Israeli espionage within the United States](#) from back in

December of 2001. Cameron's reports showed that the Mossad had penetrated high-security federal buildings and made off with top secret documents; I don't think my conjecture that the FBI was suspicious of Cellebrite's likely working relationship with the Mossad is too far off the mark.

Unfortunately for most [free software](#) advocates, the typical mode of discovering the inefficacy of some digital encryption technology is by reading court documents. Although the [judicial transparency](#) is certainly good, this is a reactive approach, and even then, it only highlights failures. Might it be time to explore other approaches in learning about the efficacy of digital encryption that is more proactive in revealing *both* the successes and failures of such ventures?

An Economic View of Cell Phone Ownership & Usage

Why have cell phones become so popular in the first place? It could be said that the lack of commercial regulations against the burgeoning telecommunications industry might explain the unbridled success of cellular service providers, but this would seem to contradict the oligopoly of Big Telecom. Generally speaking, cartels do not favor the [spontaneous order](#) of the free market with their fascist business models, so how is it conceivable that [market discipline](#) functioned so well here with the development and marketing of cell phones amongst the general public?

Much like how [inmates are able to smuggle illicit narcotics into government prisons](#), central planning can only go so far before it begins to buckle and crack under the weight of reality. Given that [knowledge is dispersed](#), the slightest deregulation of otherwise quite onerous business regulations serves to reinvigorate the entrepreneurial spirit, and when coupled with the [price system](#), this is the impetus needed for entrepreneurs to increase quality while lowering costs. Put another way, if the market is successful as it is under the most horrendous and trying of circumstances, then how much more effective would it be if those handicaps were absent?

A man's [use value](#) for cellular telephony increases the more his very livelihood depends upon it, regardless of whether digital encryption is available or not, whether user-friendly or not. The development of the [cordless phone](#), followed soon after by the hefty [car phone](#), demonstrated a growing [market demand](#) for mobility in telephony. Once the car phones became mobile enough to be battery-operated, then it was only a matter of time until they were capable of being handheld, and thus the cell phone was born.

Texting, picture messaging, and even videography (especially when coupled with Internet access), came not too long after cell phones had proven their use value across wide demographic varieties of people. It could be said that now the entire American population can be categorized in terms of their cell phone ownership and usage:

- Those who can live their lives fairly comfortably without any cellular usage at all, for it would mainly be a novelty for them since many of these folks lived most of their lives using landline phones, although it would also be fair to say that a contingent of these non-cellular users would be composed of [neo-Luddites](#) who refuse to use cell phones on principle.
- Others for whom using cellular telephony is a way to increase their social status and connectivity with friends and family; these would be the hobbyists and dilettantes who derive pure pleasure from calling, texting, and filming using their cell phones, even though their own use value for them is strictly recreational.
- A larger noticeable portion of the population began using cell phones as a way of maintaining emergency communications, as well as a way for both providers and dependents within family units to keep in close touch with each other regarding the daily routine business of life. A [latchkey child](#)'s first exposure to cell phone usage typically begins against this backdrop, given that their parents have few other options available to them that can serve to keep tabs on their children from afar.
- The supermajority of cell phone ownership is directly tied to a person's reliance upon them as the facilitator of his very own livelihood. Whether it be an employer provided phone, or one that comes out of his own pocket,

cell phone usage became ubiquitous because it enabled greater mobility in earning a paycheck. Fewer corporate staff meetings, fewer memos, and fewer progress reports to one's employer all resulted from the greater availability of an employee through his cell phone. Although this was probably the singularly greatest boom to worker productivity, the cost of it entailed keeping this relatively new device on one's person throughout the entire workday.

Granted, this is merely a sketch of how cell phone users could be conceptualized, it is simply a model for how to think about the purposeful behavior regarding the motivations driving cell phone ownership.

In passing, [Uber](#) ought to be mentioned here. This company's smartphone app has single-handedly begun real market competition against the licensed taxi monopolies strewn across America. As much as many would love the taxi monopolies to go embarrassingly bankrupt, it should be understood that Uber is, first and foremost, a ride-sharing smartphone app; obviously, this necessitates the use of a cell phone. Skeptics doubt that Uber would facilitate any form of [end-to-end encryption](#) for both drivers and customers, but at the same time, it would be most unwise to make the perfect the enemy of the good. Emergent technologies are usually built on top of preexisting ones, yet not everyone in the ride-sharing industry cares about individual privacy; so, as long as [Uber remains plausibly legal](#), then privacy is a moot point, although it is foreseeable that a market demand in user-friendly encryption could arise should ride-sharing become outlawed.

A proactive solution that could be used to incentivize the development of not just encryption-friendly smartphone apps, but also in conducting [security audits](#) of free software, would be to organize various [moneybombs](#). Tom Berson of Anagram Laboratories performed [a security evaluation of Skype back in 2005](#) when he was given access to their proprietary source code; to be sure, Ed Snowden had some very choice things to say about this VoIP & IM service provider (specifically, that [Skype became a PRISM collaborator](#) on February 6th of 2011). [Crowdfunding security audits](#) is, I think, the best way to objectively determine any vulnerabilities in free and open-source software. [Financial transparency](#) ought to be provided by the fund managers, and the hired computer programmers who examine the source code can be held accountable when they publish a white paper detailing their results, thereby enabling the release of the funds they would have then earned.

The Medical Effects of Cell Phone Usage

A [meta-analysis](#) of the currently available scientific literature revealed that there are physiological effects from the microwave radiation (MWR) emanating from smartphones. The [Journal of Microscopy and Ultrasound published a study in 2014](#), which suggested that children are noticeably more affected by MWR than adults are, simply because of their thinner skulls, relatively smaller body sizes, and more absorbent brain tissues. Although the Morgan, Kesari, & Davis meta-analytic study included other devices such as laptops, I will confine my remarks here strictly to cell phones (Bluetooth devices were not mentioned at all in these studies).

One case study showed that tumors developed in spots on teenage girls' breasts where the cell phones were sewed into their bras. Another study reported a significant risk of brain cancer in regular cell phone use by children whose median age in the study was 13 years old; a similar Swedish study largely corroborated with the significant risk of brain cancer, but also with cordless phone use. Oddly enough, a study examining cell phone use amongst *adult* men showed that cell phone usage decreased "the semen quality in men by decreasing the sperm count, motility, viability, and normal morphology." Two corroborating Japanese and Australian studies revealed that lower sperm count, decreased motility, and DNA fragmentation were all resulting from cellular MWR; the Australian scientists in particular said:

“These findings have clear implications for the safety of extensive mobile phone use by males of reproductive age, potentially affecting both their fertility and the health and well-being of their offspring.”

Another scientist, professor Stanton Glantz at the University of California’s San Francisco Medical School, concluded his own meta-analysis by saying:

“Taking all the information we have discussed on cell phones and sperm allows us to confidently conclude that exposure to cell phones adversely effects sperm.”

Obviously, the meta-analysis by Morgan, Kesari, & Davis wasn’t limited exclusively to children, but don’t necessarily think [confirmation bias](#) is at play here. The conclusion of their meta-analysis is that the risk to children and even adolescents from exposure to MWR devices is considerable, but also that adults have a very real risk, albeit a smaller one.

It is hard to argue that these studies are inconsequential, simply because they appear inconvenient to the bottom line of Big Telecom. If, indeed, the health risks are provably real and not just statistically significant, then consumers need to know that in order to make a truly informed decision as to whether the risks outweigh the benefits in choosing to own and use a cell phone. As can be expected, if your livelihood is utterly dependent upon using such an invention, then the question of whether or not such a device might put you in the midst of an [electromagnetic soup](#) seems more like an afterthought, because how else are you going to be able to pay the bills if you don’t use a cell phone?

Socio-Cultural Adaptation of Cell Phone Usage

Pew Research Center has studied the practical realities of ubiquitous cell phone ownership for years. Generally speaking, [all other forms of computer technology ownership falls behind that of cell phones](#), even laptop and desktop computers; also, the younger one’s generation is, the more likely he is to own digital electronics. Generation X and Millennials have cellular telephone ownership in the 90th percentile, at 92% & 95%, respectively.

Interestingly enough, cell phones have been reported to [alleviate boredom as well as a mechanism by which to avoid interacting with nearby people](#), and this is especially pronounced amongst Millennials. Assuming there is overlap of this with the purported [rudeness of cell phone users while on a call](#), then the spontaneous ordering of cultural norms, as determined through individual market preferences, is going to be one hell of an adventure, to say the least. As a side note, I am rather dubious as to the spread of the generational gap, since Baby Boomers, Gen X-ers, and the Millennials are all pretty socialistic, for the most part; so, whatever cultural norms may emerge, it’ll probably be based on some false notion of egalitarianism as advocated by the [“social justice” equality freaks](#).

On a somewhat more humorous note, a study conducted by Ohio State University discovered that [“distracted walking”](#) was largely correlated to pedestrians who were so glued to their cell phones that they were struck by cars while walking in the middle of the road or literally walking off bridges into ditches. Calling someone was noticeably more distracting than just texting, they also found. While this might sound rather harsh, I think these idiots deserve

all of it; think about it, if you are so “busy” that you are not paying attention to where you are *walking*, then, frankly, you deserve whatever happens to you, truth be told.

Conclusion: Options, Solutions, & the Future of Telephonic Privacy

In light of the legal, technological, economic, medical, and socio-cultural realities that cellular telephony has brought to the table, then my original question about whether cell phones are mostly beneficial or noticeably detrimental to individual liberty must now be addressed. As I said earlier in the introduction, weighing both the pros and cons of cell phone ownership necessarily entails a thorough grounding as to how such an invention has a multi-faceted significance within your own life. Security culture is only valuable to the extent that its practitioners are less vulnerable to coercion than those who fail to take their right to privacy seriously.

It must be kept in mind that **cell phone ownership is voluntary**. There is no law that individually mandates that you *must* purchase a service plan, or else you go to jail and/or face a penalty or a fine. This is *not* an insignificant detail, for it sets the stage as to what my suggestions are for dealing with this invention.

First and foremost, you could take the [Luddite](#) route. Although it would make your life arguably more inconvenient, landline and even cordless phones still exist, so any utility you demand for telephony in general can be satisfied this way, and an additional plus is that there are far greater legal protections for those types of phones; besides that, they are noticeably less intrusive against your privacy, even if the content of your calls were being specifically wiretapped by the FBI (as opposed to being indiscriminately wiretapped by the NSA).

Should you decide to use a cell phone for whatever set of reasons, then for goodness sakes, at the bare minimum, **USE ENCRYPTION**. Given the growing popularity of free software, their user-friendliness has greatly increased in recent years, so age-old excuses for not using digital encryption are going away, whether you like it or not. The most important forms of digital encryption I recommend you seriously consider are [OTR for instant \(text\) messaging](#) and [ZRTP for your calls](#); an easy to use catalog of program applications can be found on the [PRISM-Break website](#). More detailed how-to information for not only configuring these and other encryption programs onto your smartphone, but also for guidance about good information security practices while using your cell phone, are available via the Electronic Frontier Foundation’s [Surveillance Self-Defense](#) project, the Tactical Technology Collective’s [Security-in-a-Box](#) project, and the Privacy Rights Clearinghouse’s [Fact Sheets](#).

A related pair of solutions involve both Silent Circle’s [Blackphone](#) and the [Dark Android Project](#). I’m rather skeptical of Blackphone, not because I doubt Phil Zimmermann’s involvement in providing good security at all, but rather that their business model seems awfully similar to the Germanic [Cryptophone](#). If you want no fuss secure communications, then expect to pay through the nose for it to the tune of at least several hundred dollars, never mind the ongoing maintenance costs of whatever service plan you end up using. By contrast, the Dark Android Project is more in the spirit of what the [Free Software Foundation](#) promotes; what the project’s mission essentially is are attempts to construct a cell phone, either literally from scratch or from a standard Android operating system, and then configuring its apps in such a manner as to provide the maximum degree of individual privacy possible using today’s available digital encryption technology, and at a fairly nominal cost, too.

Another related pair of mitigating options are those mentioned by the “odd couple” of a police detective and a satirical alternative media vlogger. Detective Cindy Murphy’s [white paper on data extraction](#) mentioned that:

“Isolation of a cellular phone in the field can be accomplished through the use of Faraday bags or radio frequency shielding cloths which are specifically designed for this purpose. Other available items such as arson cans or several layers of tinfoil may also be used to isolate some cellular phones.

One problem with these isolation methods however is that once they're employed, it is difficult or impossible to work with the phone as you can't see through them or work with the phone's keypad through them. Faraday tents, rooms, and enclosures exist, but are cost prohibitive."

Similarly, [Montagraph's vlogs on improvised Faraday cages](#) are a direct application of what detective Murphy was explaining. Needless to say, there is also the approach of simply [removing the cell phone's battery whenever you're not making calls](#), but disassembling your phone more than once a day becomes a rather major pain after awhile, so perhaps Montagraph's approach of cost-effectively shielding your phone without disassembling the damn thing every time might be the best of all worlds here.

Ultimately, when it comes to the invention of the cellular telephone, you are going to have to make decisions involving tradeoffs between functionality and surveillance, whether the former of the two takes the form of text messaging, ride-sharing, or even using something that is still rather novel like crypto-currencies. Such decisions should not be made lightly, for your practice of security culture, or lack of it, will largely determine rather serious consequences for your freedom.

As for me, I personally regard cell phones as a tool I begrudgingly use as infrequently as possible, even to the extent of trading favors with others so I can borrow their phone in order to deliberately fail to maintain a reachable phone number, but that's just what I've been doing as of late. Perhaps over the years I'll morph into a real cellular tech-dweeb who can easily convert any Android phone into a nearly untraceable communications device that will become unparalleled in human history. [As Cody Wilson once so beautifully phrased it](#):

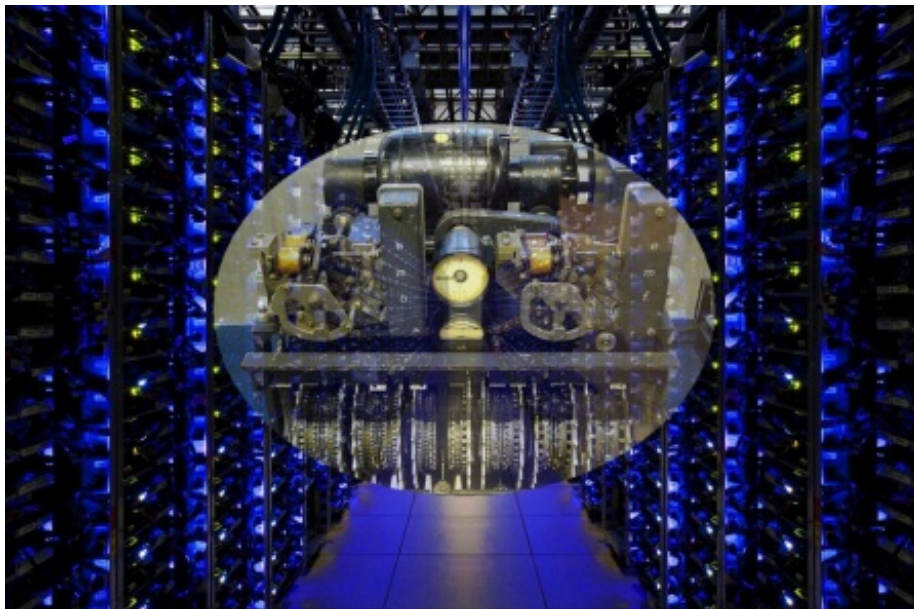
LET THERE BE DARK!

Dual Layer Encryption: A Proposal for Sidestepping Potential Backdoors

www.thelastbastille.com/2016/05/22/dual-layer-encryption-proposal-sidestepping-potential-backdoors/

*“How can we know whether someone has deliberately planted their own security hole in PGP? What if **the government** (pick any government) induced the PGP Corporation to insert a ‘backdoor’ that allows the police, FBI, KGB-reincarnated, et cetera to decrypt our messages and files with ease? The source code for various PGP versions is public. Expert computer programmers – definitely **not** employed by the PGP Corporation – can pounce on each new version and study the code carefully...[n]ot once has an alarm been raised that a deliberate weakness was inserted into PGP...[a]s a software test engineer, I must admit that code examination has its limits.”*

– [David Ross](#)



[Phil Zimmermann](#), the creator of Pretty Good Privacy, has [repeatedly denied that his creation has any backdoors](#). Despite being investigated for three years by U.S. Customs for alleged export control violations, which he was cleared of, Zimmermann’s PGP is feared by certain Americans to be compromised in some way, whether it be technologically by [the NSA](#) or by Zimmermann simply handing over such a backdoor to the federal government. Last time I checked, in *this* country there is such a thing as the presumption of innocence before being *proven* guilty, not the other way around; folks who care about strong cryptography ought to give Zimmermann the benefit of the doubt by taking him at his word.

As an advocate for PGP, I have encouraged people to learn about the [history of PGP](#) as well as [how to configure it with their email clients](#). Most grumbling I’ve come across while assisting others set up PGP over the years usually stems from individuals who are reluctant to use email clients at all, because they enjoy the convenience that comes from using webmail they access via their chosen Internet browser. If they could, they’d prefer to spend Federal Reserve Notes on smartphone apps rather than spend 15 – 20 minutes downloading and using [free and open-source software](#).

Yet, what if, on the off chance, the NSA inevitably will install their own backdoor, if they haven't already, given their cryptanalytic capabilities? Should that be the case, what then? One solution, I think, to that concern is what could be called dual encryption.

Three or four years ago, [Gary Hunt](#) expressed to me that he had no faith in the Internet being a secure haven for private communications, as he had expressed in his article, [How Dangerous is Internet Communication to Patriots?](#). He then told me that he had conceived the idea of dual encryption. His idea was to blend high-tech with low-tech cryptography into a very practical high security tool. He never wrote about dual encryption because he figured that his idea would spread organically from peer-to-peer.

What is dual encryption? Simply defined, it is a form of [multiple encryption](#) whereby one layer of encryption is digital whereas another layer uses a [classical cipher](#). Digital encryption would be something like [PGP for email](#), [OTR for instant messaging](#), or [ZRTP for VoIP calls](#). By contrast, classical cryptography entails the use of [transposition ciphers](#), [substitution ciphers](#), [one-time pads](#), or other readily available ciphers.

The purpose of dual encryption is to frustrate cryptanalysts by tricking them into believing that even if they managed to crack the digital encryption being used, it becomes a moot point simply because what they perceive to be a cracked [plaintext](#) is in fact the [ciphertext](#) for the next layer. As such, until they crack that next layer, the "plaintext" they have cracked will just be unintelligible garbage.

So, what would dual encryption look like in practice? If an original message's plaintext was something like:

meet me at the docks seven pm on march twenty-third

Then the first encryption layer would be to utilize a classical cipher; for this hypothetical scenario, I'll use the easily crackable [Caesar cipher](#), shifted five spaces where A = E, just for the sake of demonstrating [proof-of-concept](#) (not for real [information security](#), of course). The ciphertext would appear as:

Qiix qi ex xli hsgow wizir tq sr qevgl xairxc xlnvh

Of course, this first layer must not be done on a computer with an Internet connection, for purposes of INFOSEC; instead, it ought to be done using graph paper.

Next, the second encryption layer would be to send that ciphertext through a digitally encrypted medium. For this scenario, PGP will be used (**note**: the following is *not* the actual encrypted message, but was copied from a webpage, and is shown here for visually conceptual purposes only!):

Now, the recipient of this dual encrypted email will need to decrypt both layers in order to read the original plaintext message about where and when the rendezvous is to occur.

First, the PGP encrypted email will need to be decrypted using [public-key cryptography](#); once that's done, then the recipient will see the ciphertext for the second decryption layer. Upon using the Caesar cipher correctly, he'll then learn the details of the meet up. Obviously, if the sender's original plaintext message can be read by the recipient, then the dual-layer encryption method has been used successfully by both parties.

To simplify the two layers on both the sender's (encryption) and recipient's (decryption) ends, here is how they are equivalent:

- Encrypt layer one = decrypt layer two (classical)
- Encrypt layer two = decrypt layer one (digital)

Naturally, everything the recipient does is what the sender did, except in reverse order. It could be argued that dual encryption increases the possibility of a honestly innocent mistake being made during either encryption by the

sender or decryption by the recipient, thereby making the communication impossible, yet that is the risk you incur should you choose to use this method. If anything, that would be a selling point for why practicing dual encryption ought to be done *before* it's actually needed.

Additionally, if the “paper-and-pencil” classical cipher you end up choosing to use requires a key, then that key should be relayed through a non-digital communications medium, whether it be something like a [landline telephone](#) or a [dead drop](#). Not only that, but overly frequent practicing might give your adversaries (such as the feds) the means to crack your cipher of choice. Therefore, only practice enough in order to assure that your working knowledge of your chosen cipher is accurate and functioning properly; be sure to **burn** all graph paper once you have finished practicing.

Dual encryption is a proposed solution to the possibility of a secret backdoor to any sort of digital encryption protocol, whether presently or in the future. Cryptanalytic [white hats](#), as well as members of the [American Cryptogram Association](#), are encouraged to see if they can discover any [single points of failure](#) or any other weaknesses in this method, and either share them in the comments section below or [send me an email](#) [[PGP public key](#)]. Any further developed proof-of-concept that shows dual encryption's viability better than I have done here would be sincerely appreciated.



Click the image to see it clearly.

How to Configure & Use PGP Encryption for Email (Mac OSX Instructions)

 www.thelastbastille.com/2013/01/18/how-to-configure-use-pgp-encryption-for-email-mac-osx-instructions/

[Pretty Good Privacy](#) (PGP) is a type of digital mail encryption program. Email that is sent over [the Internet](#) is akin to a postcard, in that any third-party who intercepts it can read the message. Encrypted email is analogous to a letter sealed inside of an envelope; while it is still possible for third-party interception to know whom the senders and receivers are (as well as the content of the subject line), they cannot read the message itself. PGP uniquely combines both private *and* [public key cryptography](#) to provide the best possible “envelope” for your email communications.

In regards to privacy, you should keep a few items in mind when using PGP. Despite PGP encryption being *still* legally regarded by the central government as a *munition*, [it is now exportable to other countries](#) (provided they are not on the list of countries, groups, or even individuals subject to [US export controls](#)). The very use of PGP itself *might* attract digital surveillance by agents of [the State](#), since even if they didn't have a backdoor, they could still tell that you wanted to prevent at least casual decryption of your messages by third-parties; of course, if more people used PGP that would it make it that much harder for government snoops to surveil *anyone*.

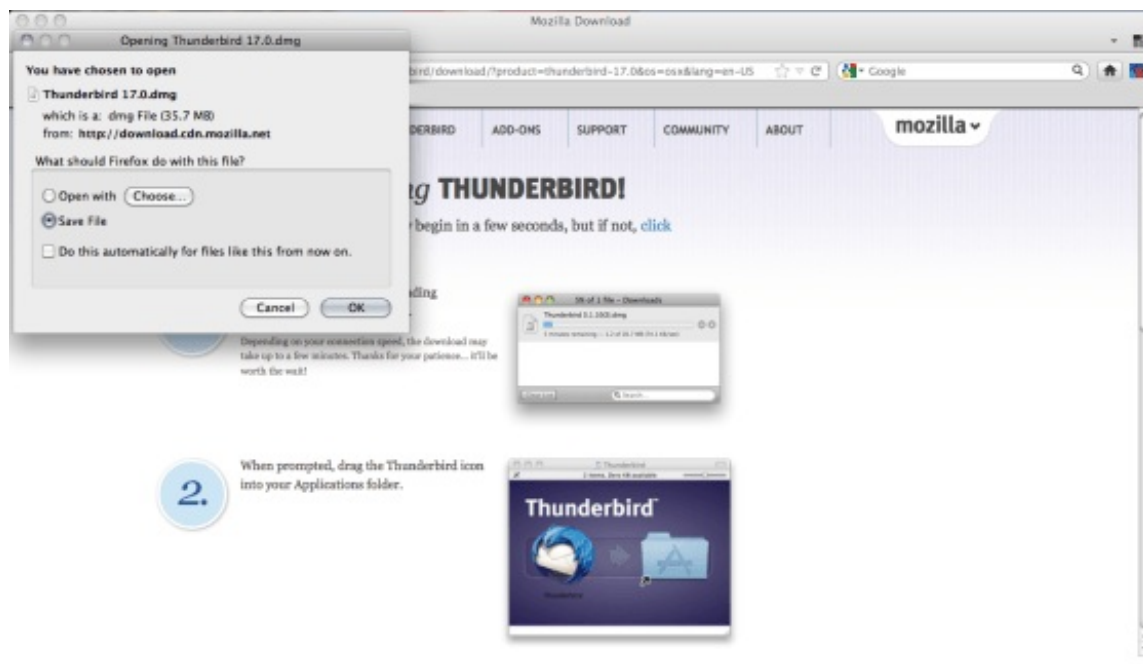
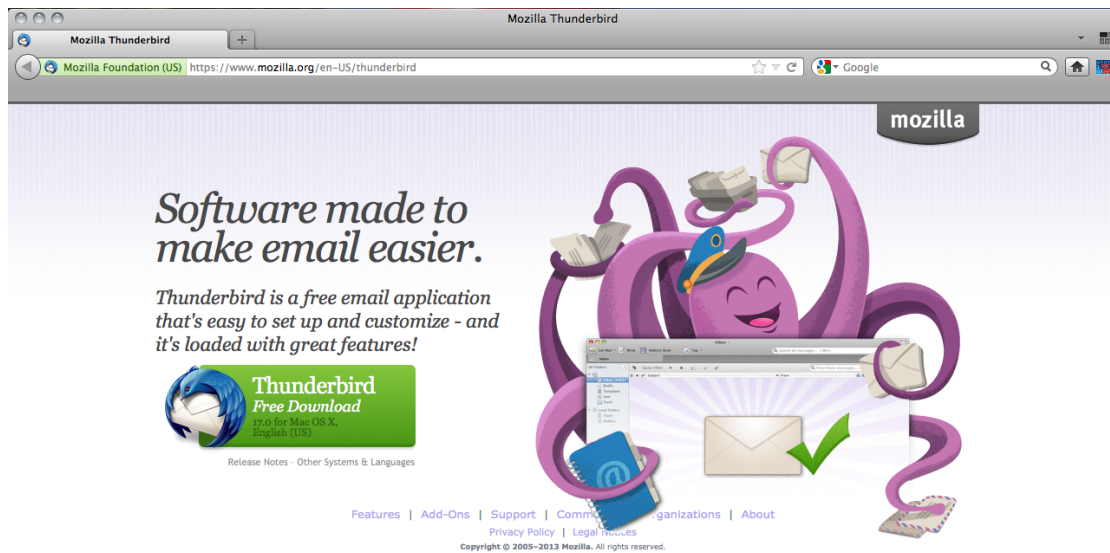
While some PGP users would suggest that all users *always* use PGP for *every single email*, this is not always possible, whether because a user needs to communicate with an individual who refuses to use PGP, or because an email is being sent to a public email list anyway. Finally, you'll need to consider how you and your contacts will exchange each of your public keys with each other (sending them in the form of a PGP key block or as an ASC file attachment via email is the least desirable, although there are a combination of digital and offline methods that can be pressed into service to provide at least a semi-secure transfer of the keys).

The following tutorial will demonstrate how to configure PGP for the [Apple Macintosh operating system](#) using the [GNU Privacy Guard](#) (which is the [free and open source software](#) implementation of the [OpenPGP standard](#) as developed by the [Free Software Foundation](#)), the [Thunderbird email client](#), and the [Enigmail plugin](#) for Thunderbird. Any other combination of software and operating systems are not applicable for this particular set of instructions (if you want to install PGP for the Windows OS, [you need to view this set of instructions instead](#)).

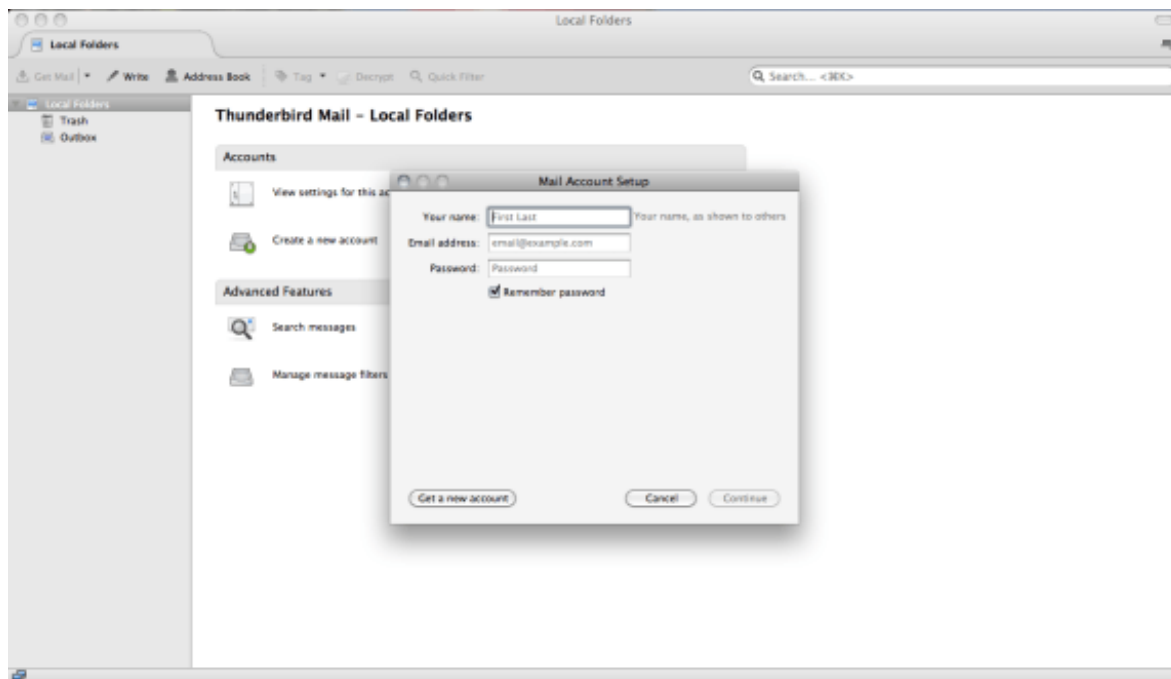
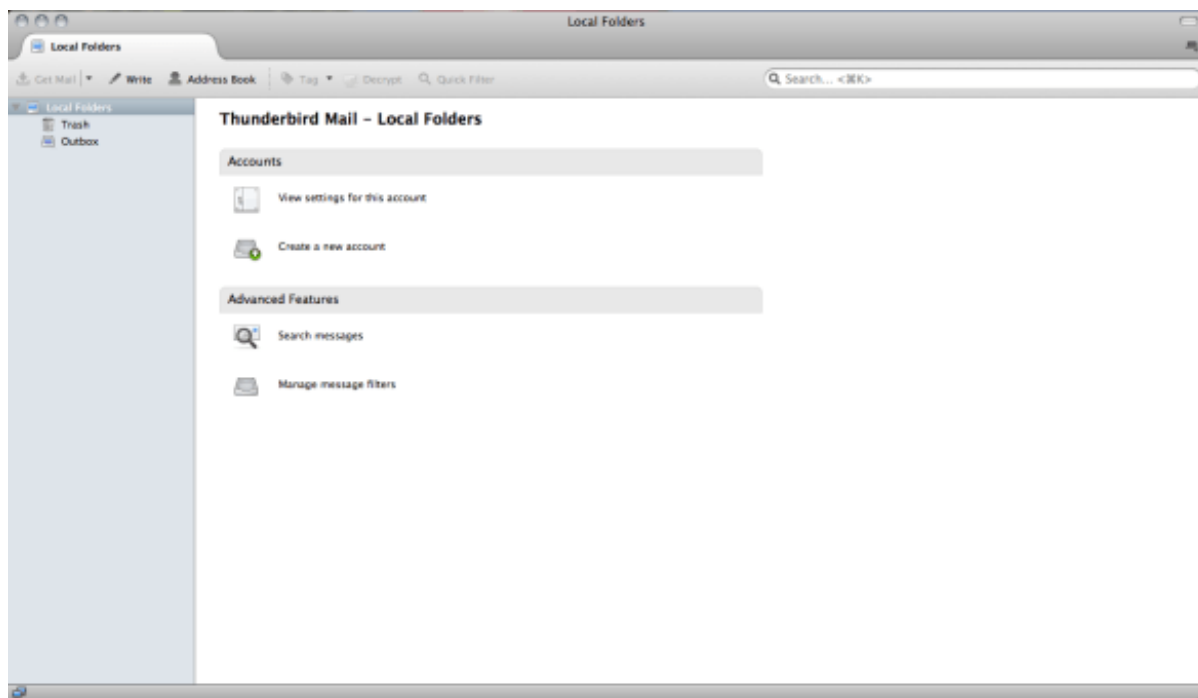
The PGP Encryption Installation Guide

Before you get started, make sure you first have 1) a reliable Internet connection, 2) a good browser, and 3) an email address that uses a [webmail provider](#) (preferably one that uses [POP3](#)) that you would like to allocate for PGP encryption.

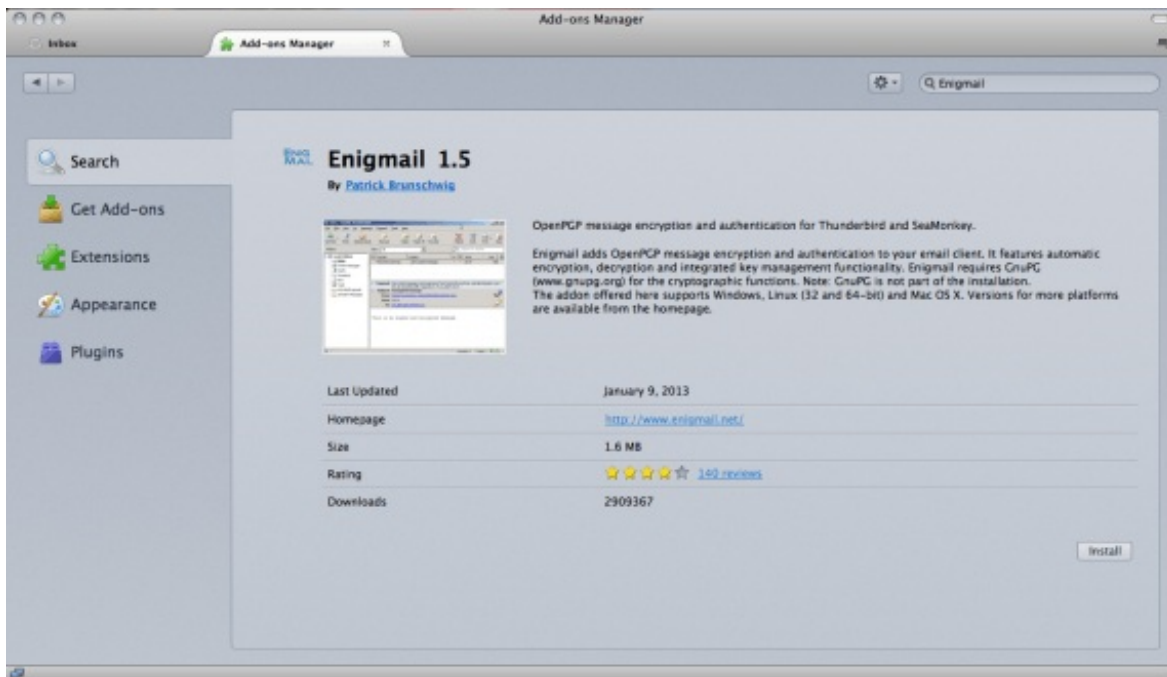
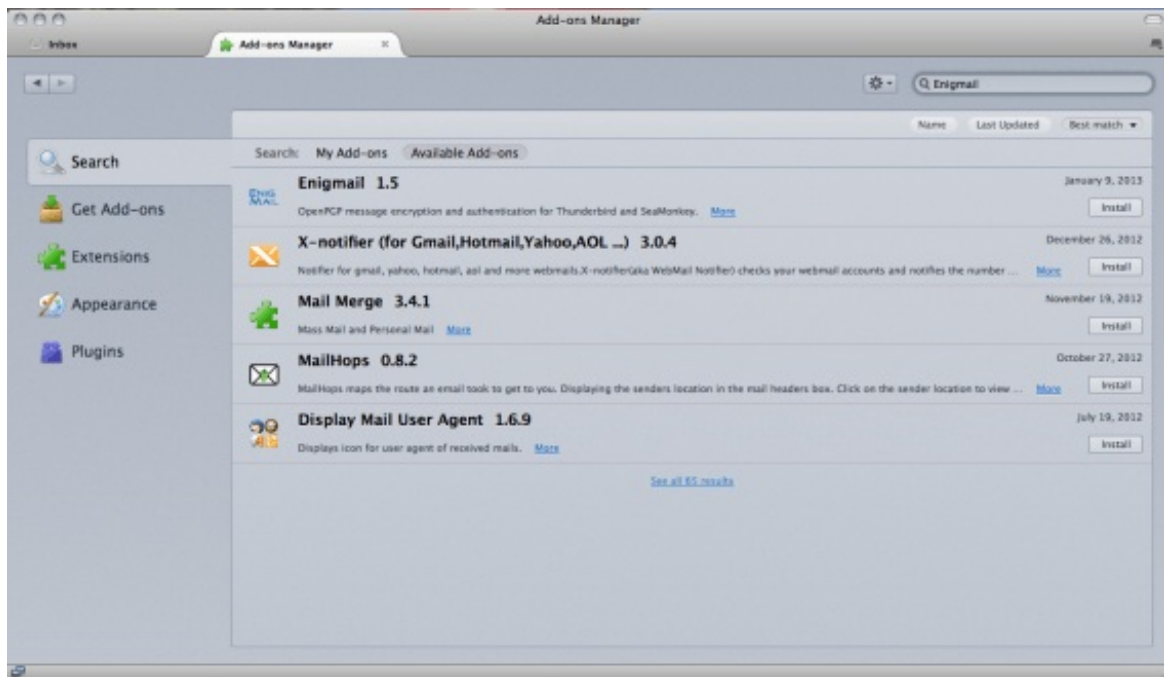
Step 1: Download the [Thunderbird email client](#).

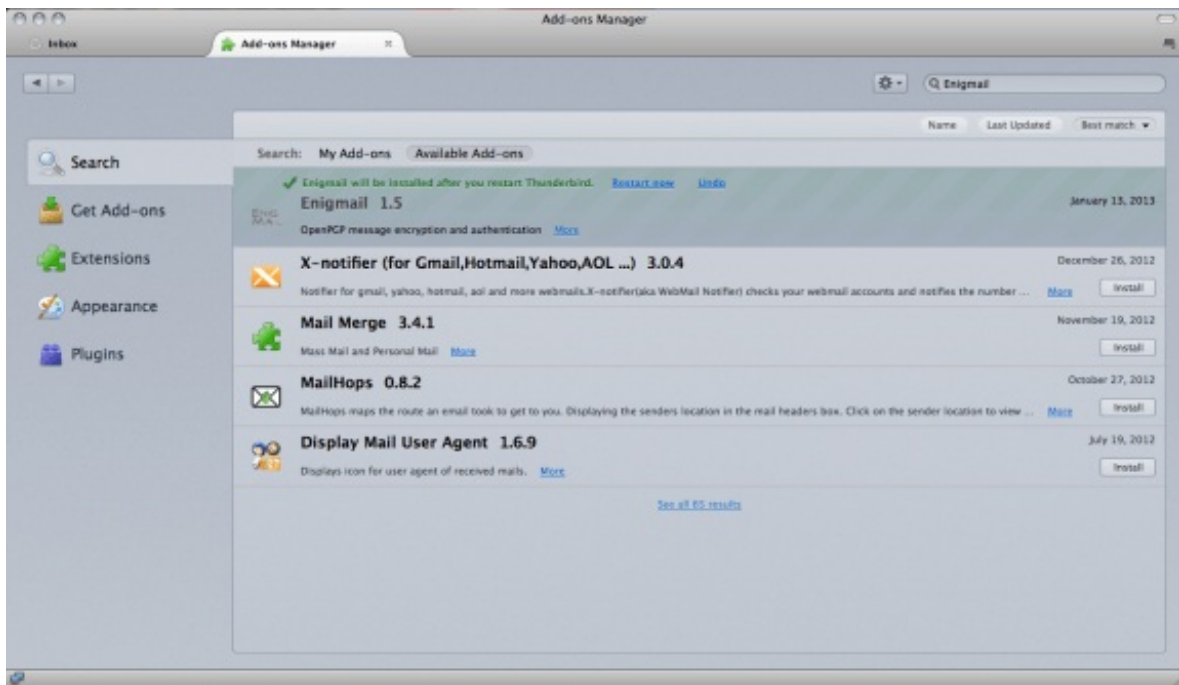


Step 2: Configure the email address you want to use with Thunderbird.



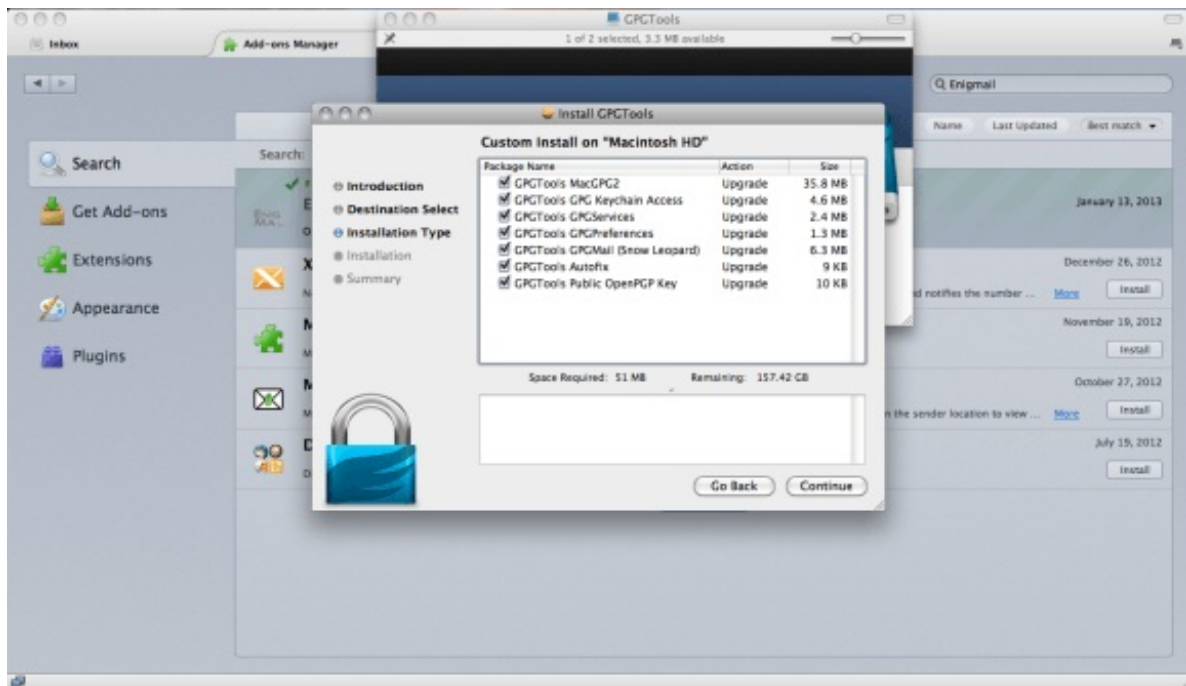
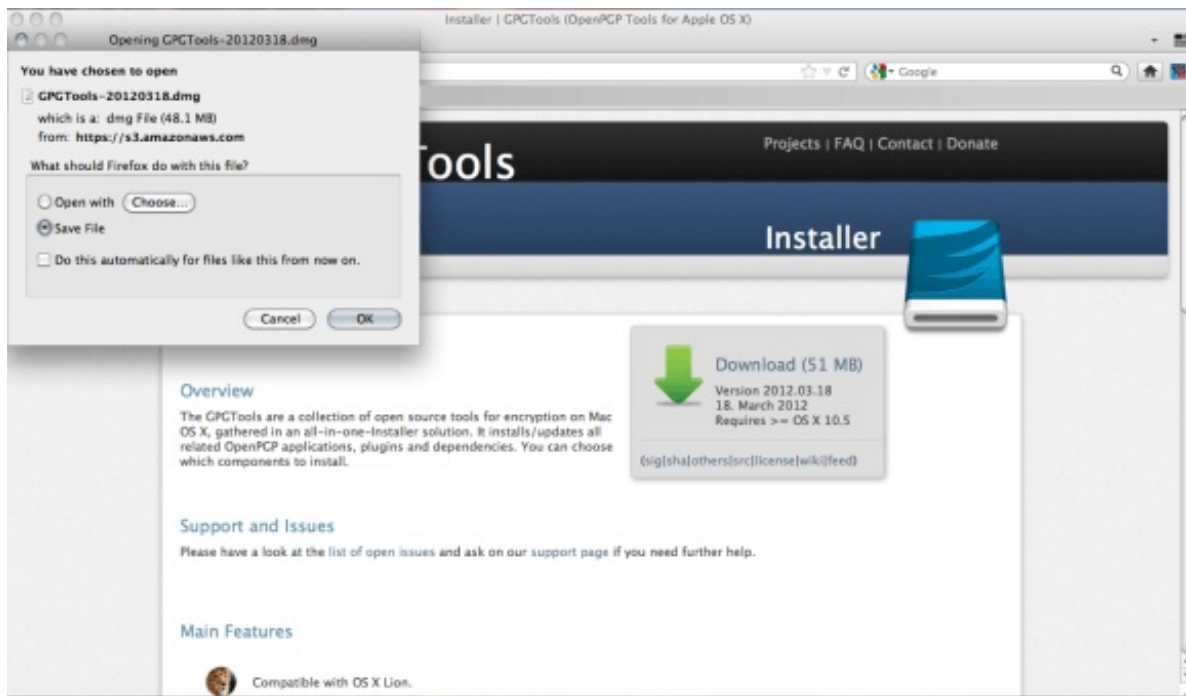
Step 3: Download and install the Enigmail plugin *through* Thunderbird (look for “Add-ons” under the “Tools” [menu bar](#)).

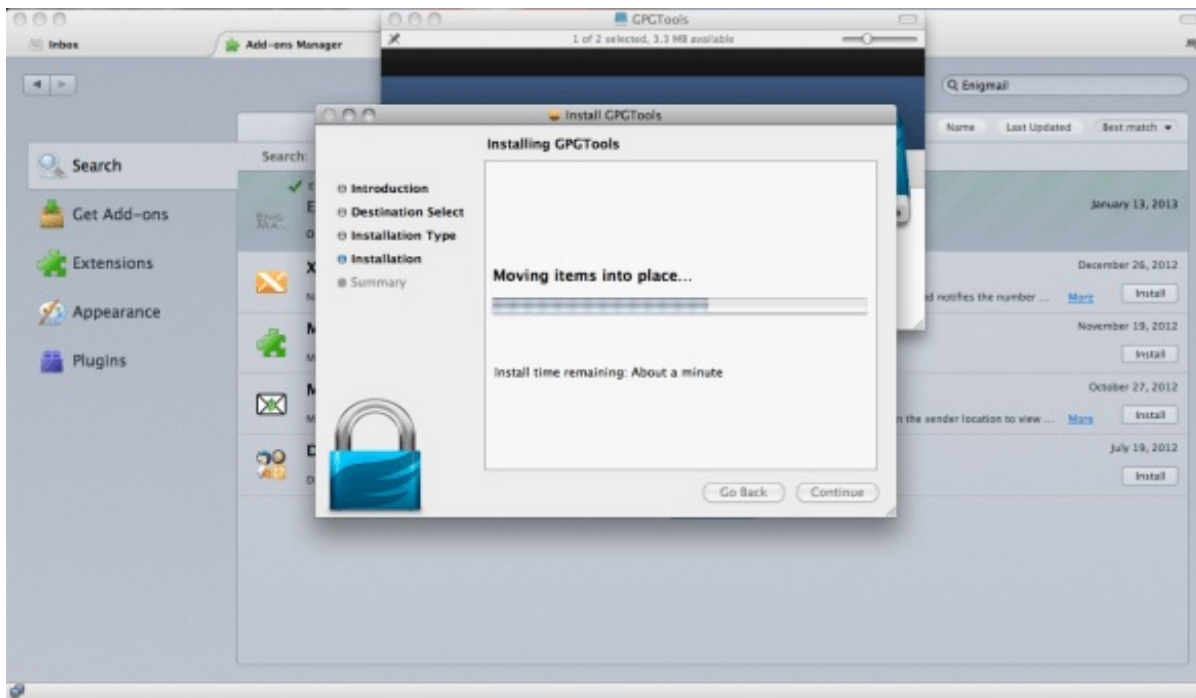




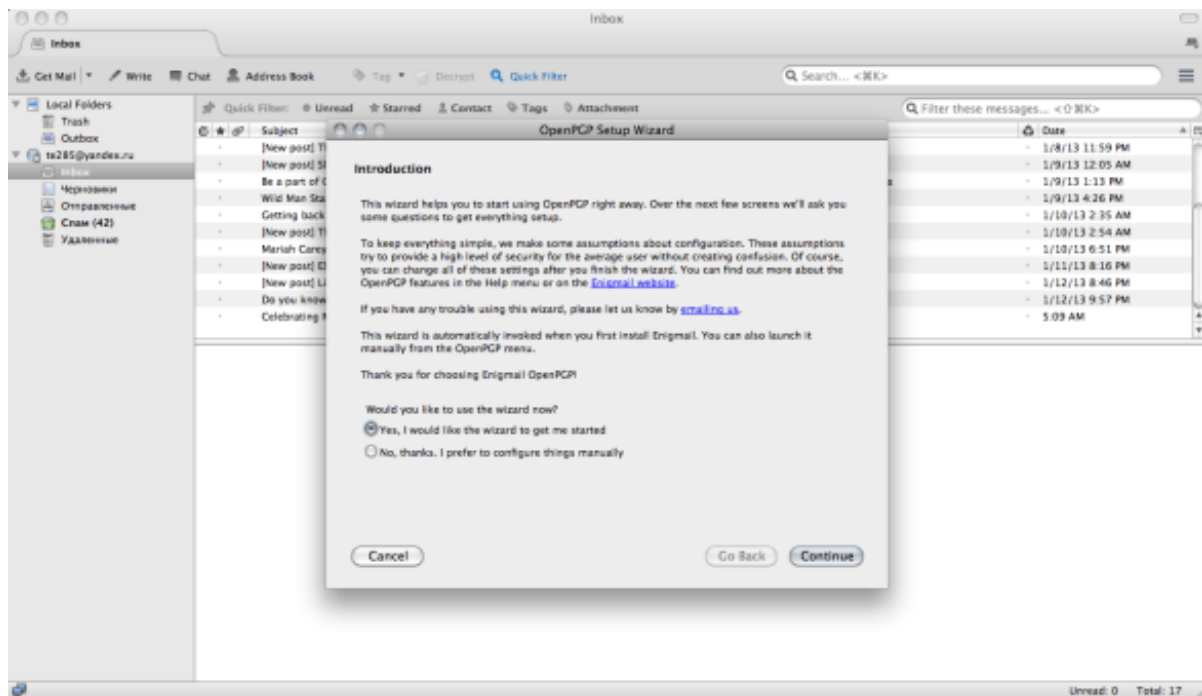
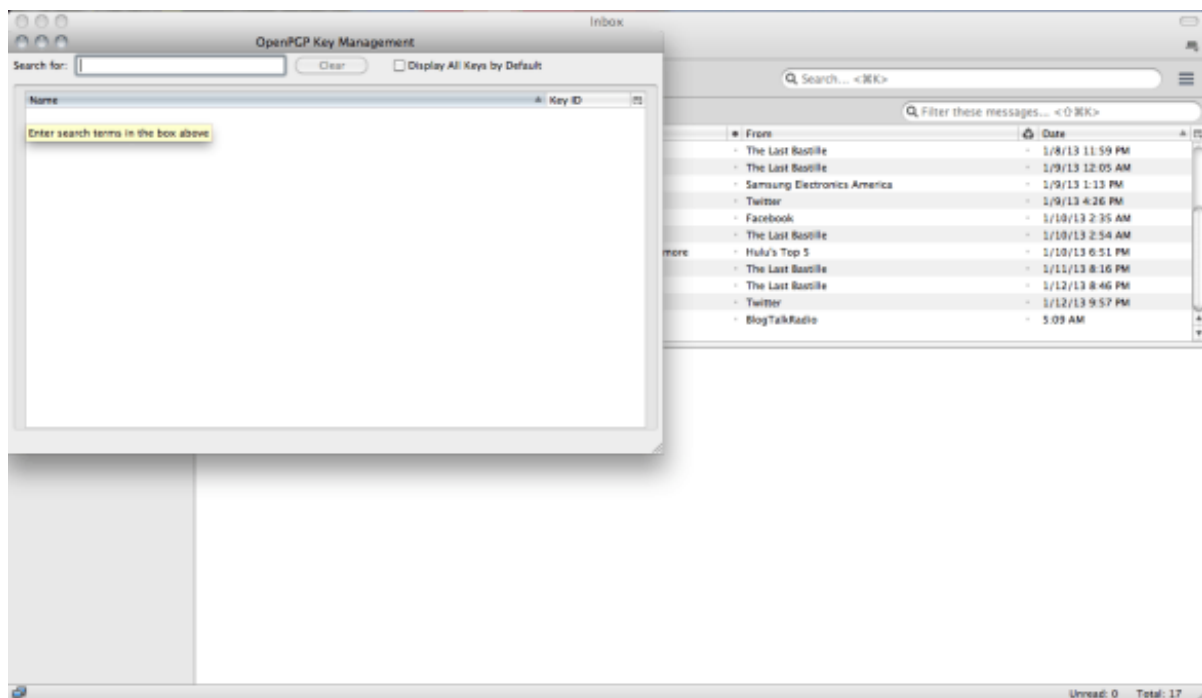
Step 4: Download and install [GPG Tools](#).

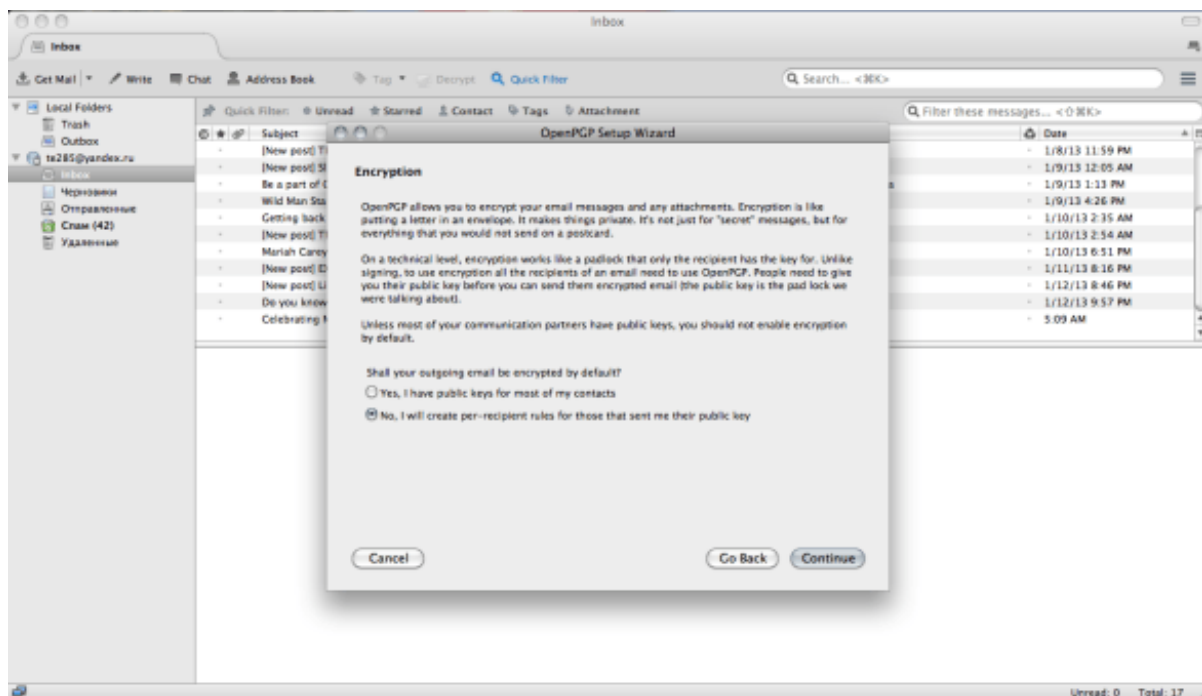
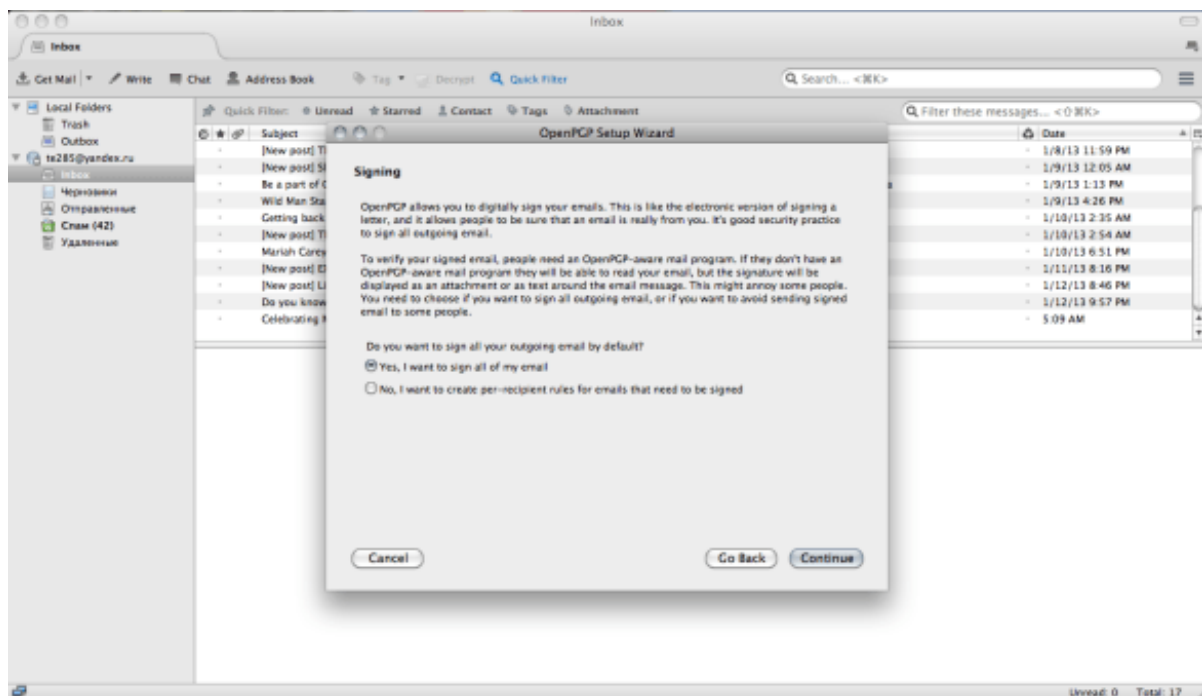


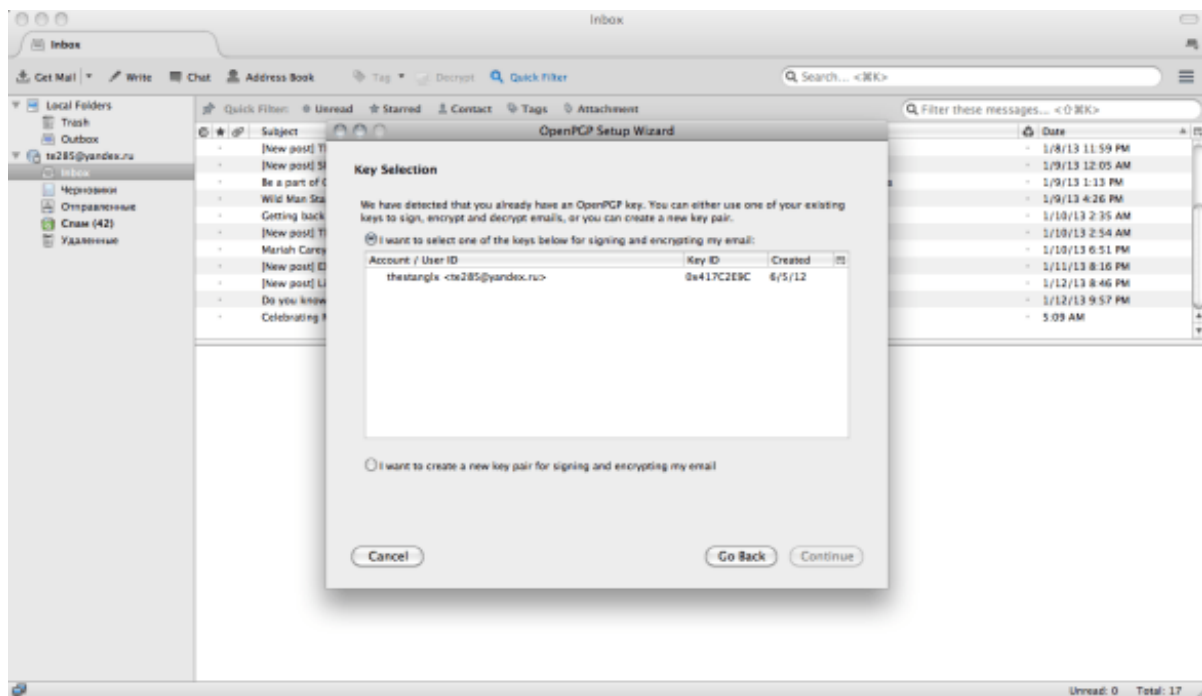
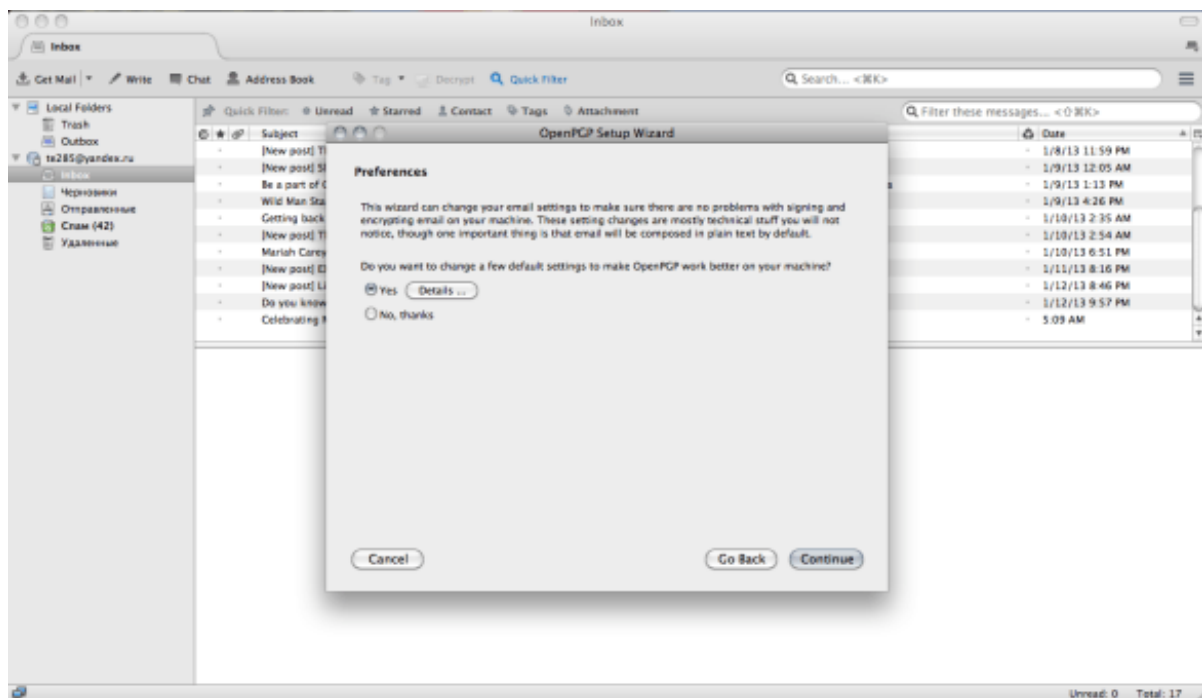


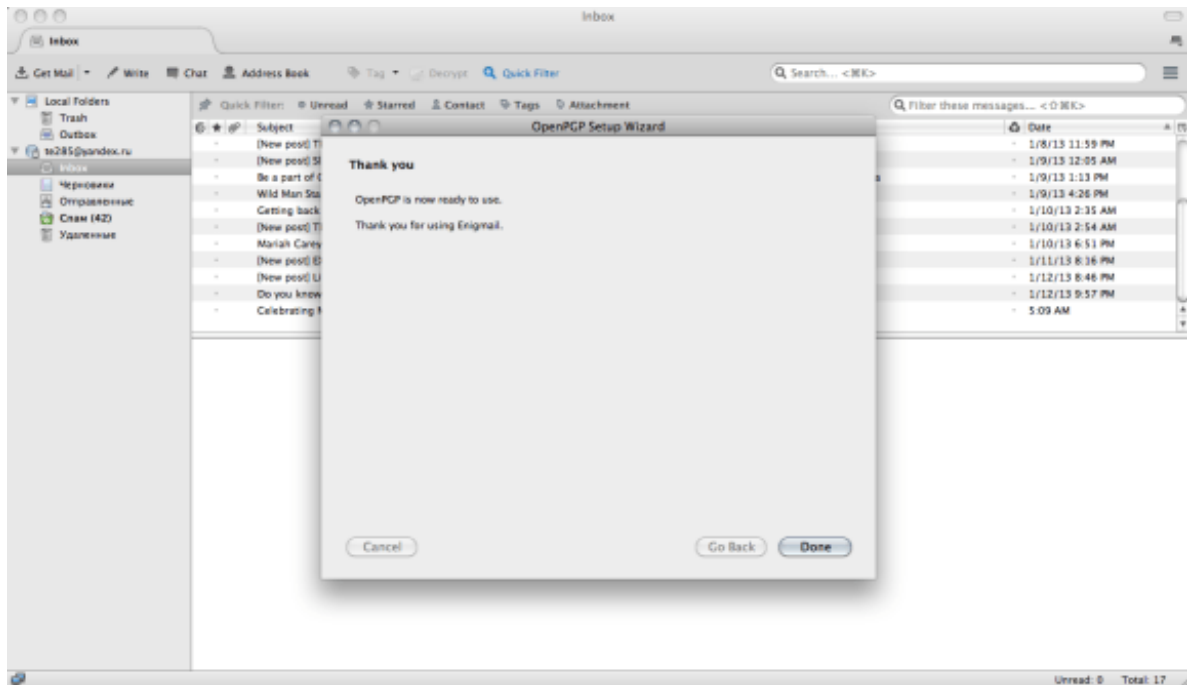
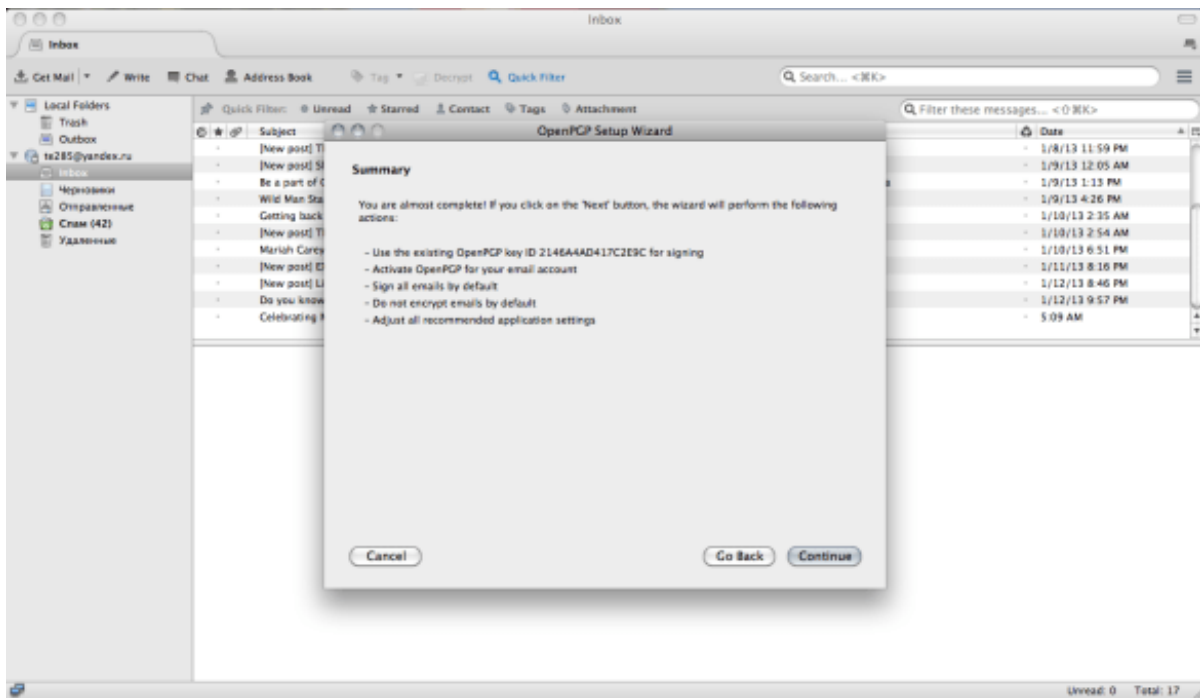


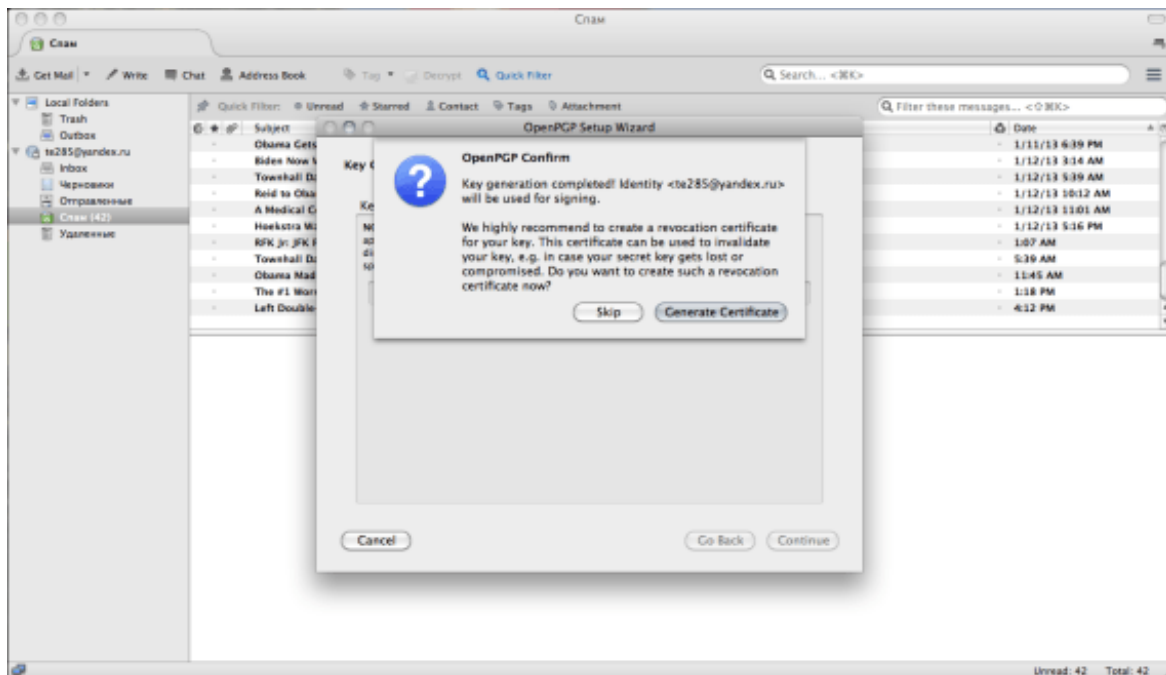
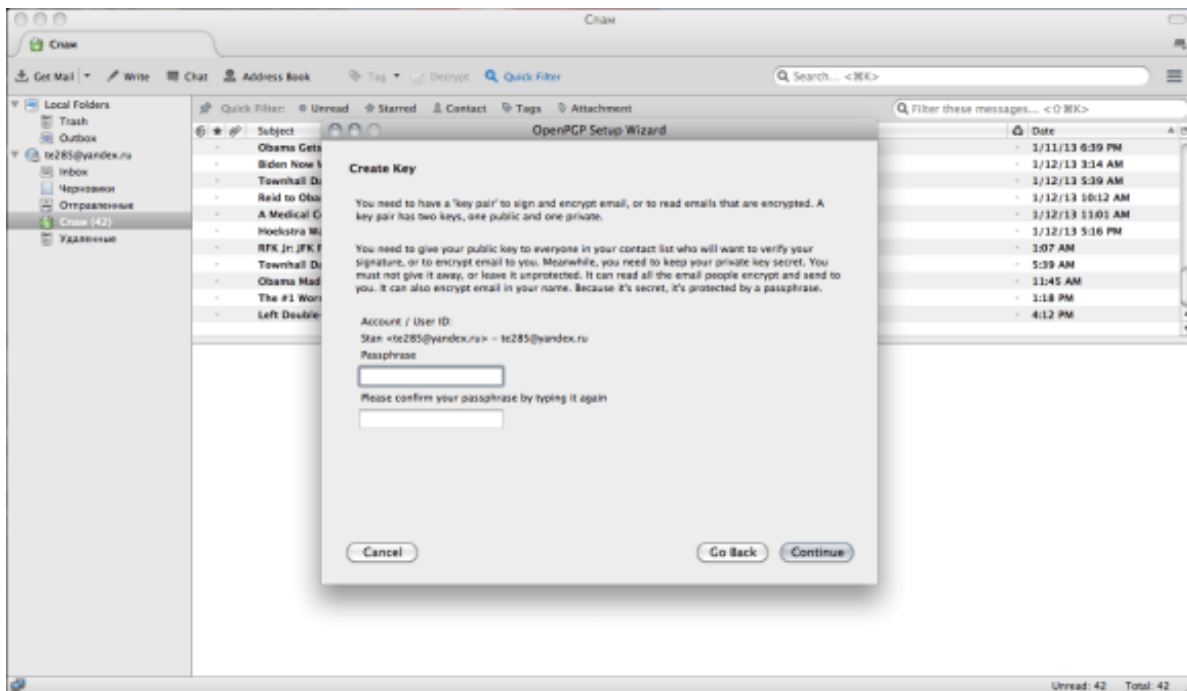
Step 5: Create a key pair (which constitutes a public key and a private key) by using the same email address you configured with Thunderbird and choosing a [passphrase](#) that you would be comfortable typing every time Thunderbird prompts you, so that you can read your encrypted emails. While you could use [GPG Keychain Access to create the key pair](#), the screenshots below show you how to do the same thing with the OpenPGP Setup Wizard (look for “Setup Wizard” under the “OpenPGP” menu bar).



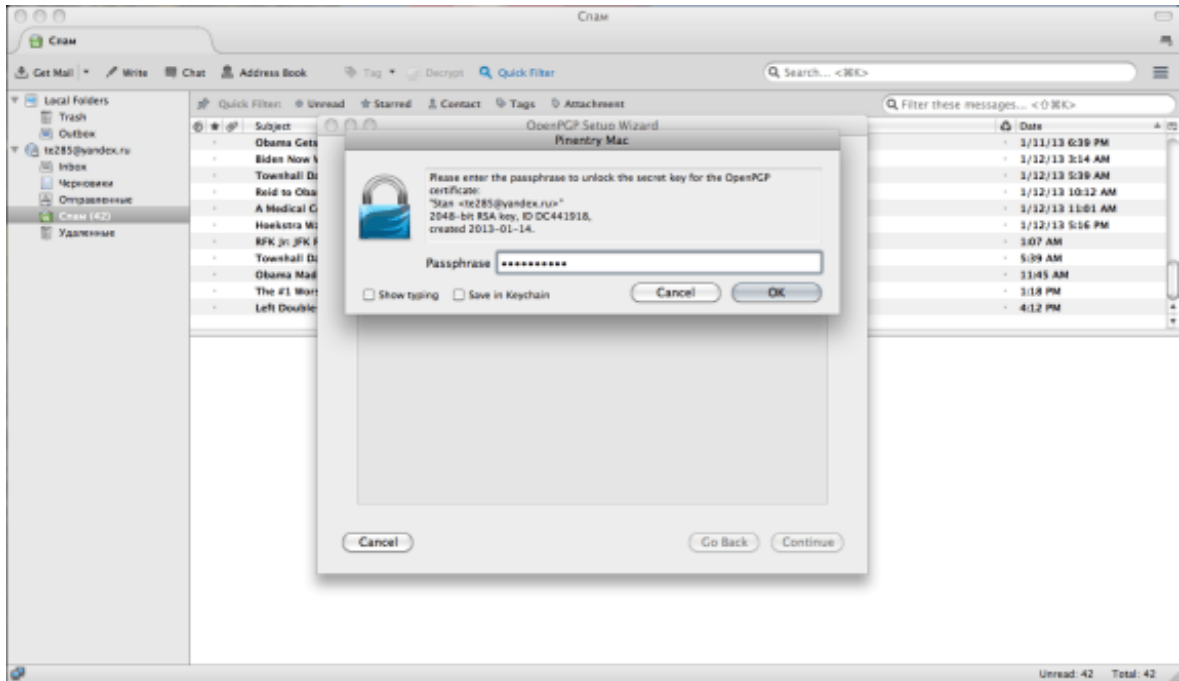
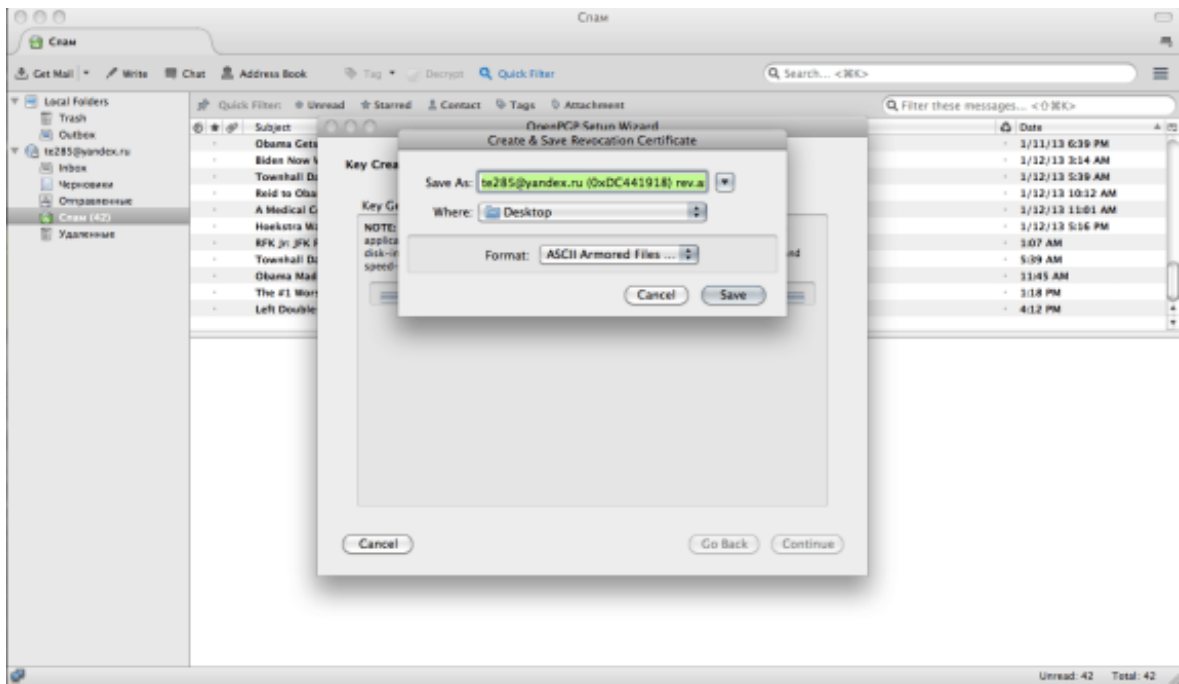


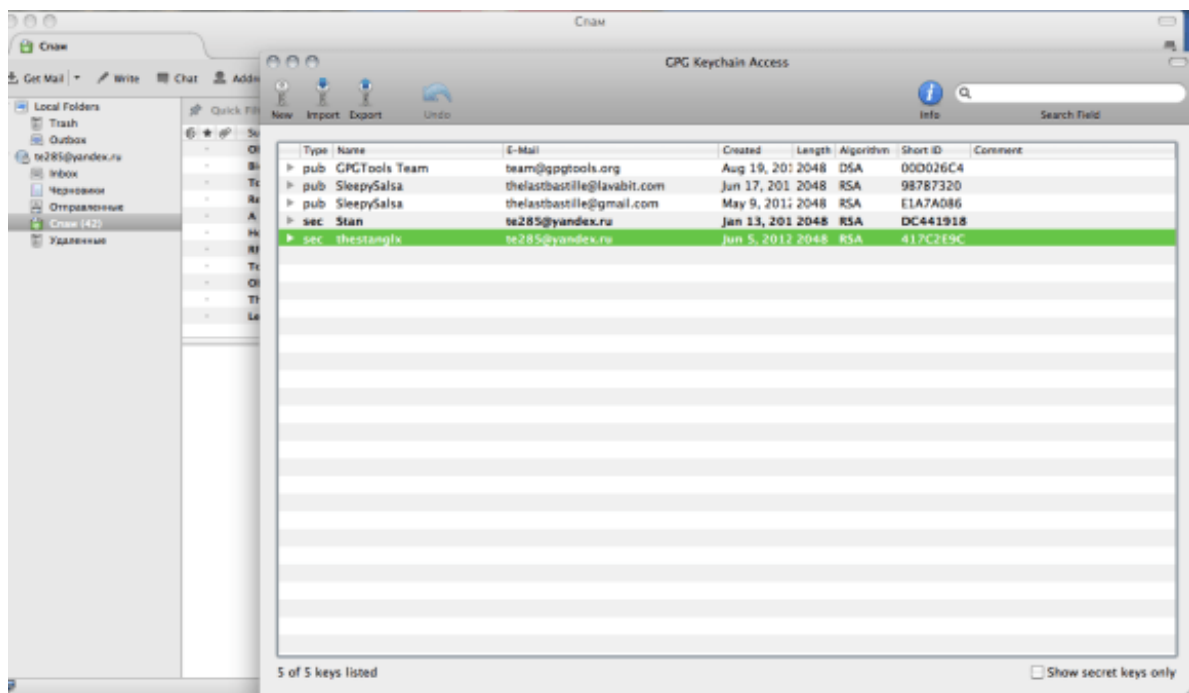






Step 6: Export your public key and keep it on your hard drive as well as another copy on at least one [USB flash drive](#) (for the GPG Keychain Access method, simply highlight the key by clicking on it, then click “Export,” and then choose where to save the ASC file).





Step 7: Find another individual who has completed the previous steps and exchange each of your public keys (preferably by trading the exported ASC files, instead of the PGP Public Key Block text). Once each of you have imported each other's public key into the GPG Keychain Access application and/or the OpenPGP Setup Wizard, then each one of you should send the other a test encrypted message just to make sure you have configured everything correctly (this is best done in person or over the phone, the latter of which either by landline, cellular, or VoIP).

Congratulations, you've successfully installed PGP; now you can send and receive encrypted email. If you'd like additional technical support with installing PGP as per this specific combination of software on a Mac OS, then feel free to [send me an email](#) (additionally, if you'd like to test whether you configured PGP correctly, also feel free to use my [PGP Public Key](#), but remember, I'll need yours first), preferably with the subject line "PGP Configuration Help." If you would prefer some additional guidance with using GPG Keychain Access, I would suggest you watch the "[GPG Encryption Software for Mac](#)," "[GPGTools Screencast](#)," and "[Adding GPG to Services/Encrypting/Decrypting on a Mac](#)" video tutorials.

How to Configure & Use Jitsi (Windows OS)

By: Shane Radliff

May 25, 2015

Jitsi is an open source platform similar to Skype and handles messaging, audio calls, and video calls. In addition to that, Jitsi comes stock with Off the Record (OTR) and Zimmerman Real Time Protocol (ZRTP) to provide secure communications.

OTR is the program used to encrypt messaging, while ZRTP is what encrypts VoIP (Voice over Internet Protocol) calls.

Since Jitsi comes stock with OTR and ZRTP, the install is quite simple; but to ensure simplicity and accuracy, I have decided to do a tutorial for the configuration and use of Jitsi on a Windows OS.

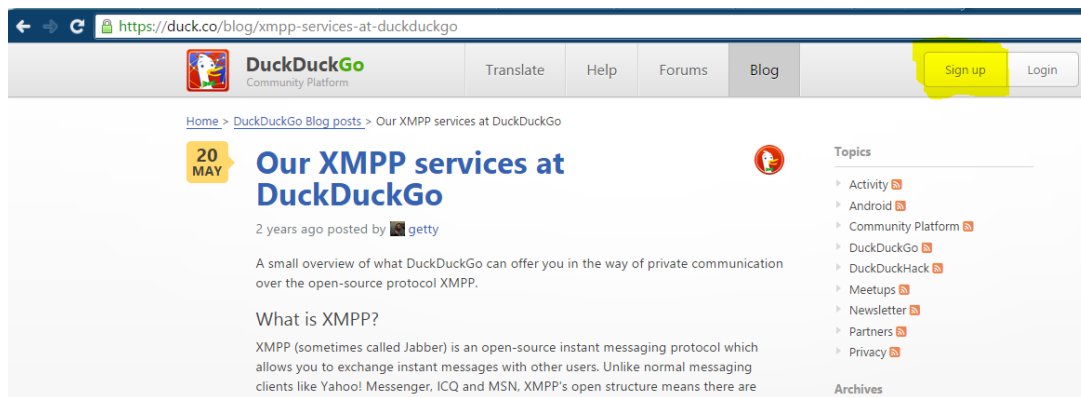
Note: I don't think the set-up for Windows vs. Mac is much different, so it's possible you could use this for Mac OS too.

Downloading Jitsi and Setting up the XMPP Server

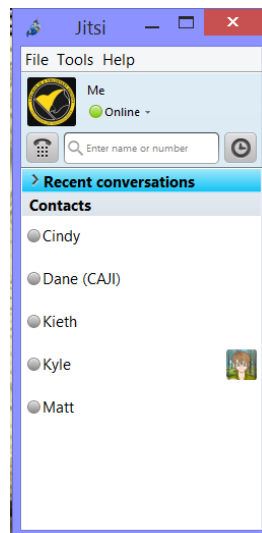
1. The first step is to download [Jitsi](https://jitsi.org).



2. While you're waiting for Jitsi to download, you'll need to set-up an XMPP server. Head over to [DuckDuckGo](https://duckduckgo.com) and sign-up. Note: make sure to remember your email (xxxx@dukgo.com) and password as you will need that to log-in.



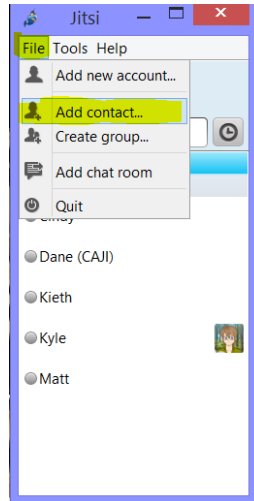
3. After you have set-up your XMPP server through DuckDuckGo, you'll need to open Jitsi.



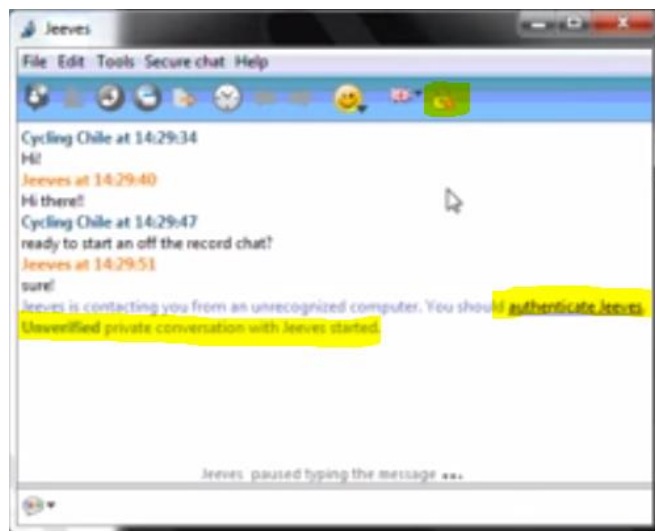
4. Once Jitsi is open, you'll click "File" and then "Add New Account". It will give you a few options but you'll want to login through the XMPP Server option (near the bottom of the list). You'll use the log-in information that you signed up with on DuckDuckGo. Note: the email will be something like: xxxx@dukgo.com.

Setting up Off the Record (OTR)

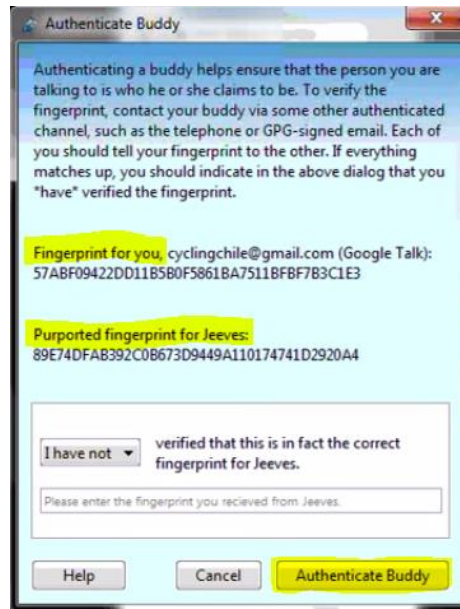
5. Next, find a buddy and add them. You'll do this by selecting the "File" dropdown and clicking the "Add contact" button.



6. Once you two are friends, you'll need to highlight their name and click the message icon to start a conversation. Next, you'll click the lock in the top right of the chat box. A dialogue should appear that states: "John Doe is contacting you from an unrecognized computer. You should authenticate..." You'll then click the hyperlink to authenticate your buddy.



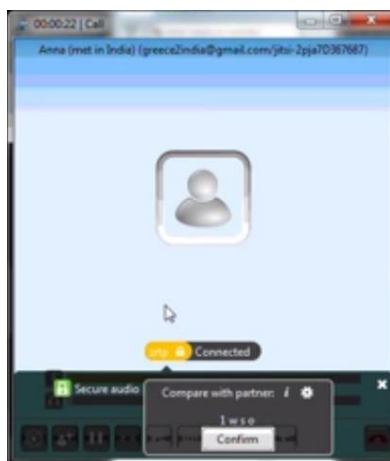
7. Once you click the link, a new window will appear. It will show your fingerprint and also the purported fingerprint of your buddy. At this point, you will have to use a separate channel to authenticate. That can be done by a VoIP call, phone call, or in person. You'll read your fingerprint and then your buddy will read theirs. If they match, then you will click "Authenticate Buddy".



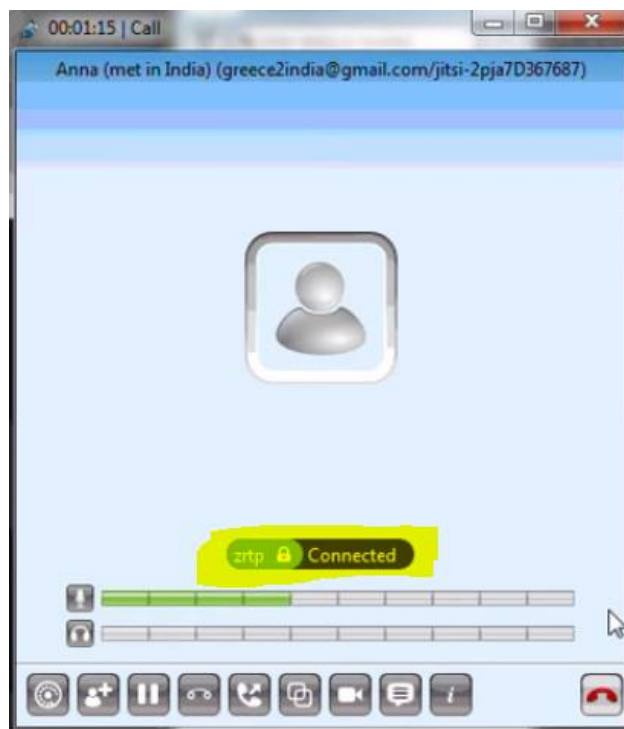
8. After you click “Authenticate Buddy”, check the chat window and make sure the lock is green and has no further warning messages. If it’s green, you’re now using Off the Record encryption in your messages with the buddy you verified. Note: keep in mind, you’ll have to do it separately for everyone you chat with, but you will only have to do it once for each.

Setting up Zimmerman Real Time Protocol (ZRTP)

9. Highlight your friend’s name and click either the audio or video call button. It will take a few seconds for it to connect and then it should start ringing.
10. At that point, you will see a button in the middle of the call window that says “connected” with an unlatched lock. That is indicating that ZRTP is not connected.
11. After a few seconds, there will be window that opens up at the bottom of the call window.



12. At this point, the call is still not secure, and you will need to verify the key with your friend as an additional security measure. If the codes match, then you will click “confirm” and close out of that window. ZRTP should be connected and you can verify that by making sure the lock is now closed and green.



If you made it through all the steps and followed the instructions, you should have Jitsi, ZRTP, and OTR configured. If not, and you're having some problems or technical difficulties, please take a look at these [two videos](#) and they should be able to answer any questions. If for some reason those do not, please [email me](#) or call me at 309-533-7857 and I will assist you with getting it configured properly.

You've just taken a great step in ensuring private communications and have also began implementing a security culture.

I would further recommend encrypting your email as well. A colleague put together a great tutorial on setting up Pretty Good Privacy (PGP), which you can find [here](#).

Lastly, if you feel like there is something missing in the tutorial or that something needs to be explained better, please let me know. This will be updated as needed when I get feedback.

[My Public PGP Key](#)

Section II:

Information Security

Socialist Insecurity: How the Raw Deal Enslaved Americans

□ www.thelastbastille.com/2015/12/29/socialist-insecurity-how-the-raw-deal-enslaved-americans/

The ideal of evolutionary biology is that parents would value the survival and betterment of their children above their own. In reality, however, parents vacillate between their own individual self-interests and those of their children, often resulting in either negotiated compromises or authoritarian dictates. Government central planners have legalized intergenerational parasitism through the mechanizations of [taxation](#) and [welfare state](#) subsidies in order to encourage senior citizens to directly feed off the productivity of the current workforce, thereby [balkanizing](#) the young and the elderly against each other.

Two concepts are helpful for analyzing the political topic of [Social Security](#). The [Hegelian Dialectic](#) shows how the pattern of “problem-reaction-solution” is used by Leviathan to further solidify its power, yet, [Hanlon's razor](#) says that malice should never be attributed to that which can be satisfactorily explained by stupidity. These two ideas will be used during this examination of the history, legalities, economics, and the privacy implications of [social insurance](#) in order to measure its compatibility with human liberty.



An Overview of the Relationship Between Central Banking & Social Insurance

Central banking, through methods such as [fractional reserve lending](#), directly causes all manner of [financial crises](#), thus beginning the formulaic Hegelian Dialectic. The [Second Bank of the United States](#) precipitated the [Panic of 1819](#) by about three years, yet this relationship was conveniently forgotten during the [Panic of 1907](#), which itself was caused by then-Treasury Secretary Leslie Shaw [stimulating inflation since 1905](#). This 1907 panic was used as the pretext for the establishment of the Federal Reserve Bank, which has since then proven itself to be incapable of accomplishing its *stated* objectives, to be a cartel operating against the public interest, as the supreme instrument of usury, the generator of inflation, a [war-monger](#), a destabilizer of the economy, and most importantly, as [an instrument of totalitarianism](#).



With the passage of the Federal Reserve Act in 1913, it would only be a matter of time until [malinvestment](#) by the Federal Reserve resulted in the [Crash of 1929](#), given that [business cycles](#) are a completely artificial phenomenon caused by excessive [credit creation](#) by central bankers, which inevitably leads to a [credit crunch](#). As former Federal Reserve chairman [Ben Bernanke said back in 2002](#):

*“Let me end my talk by abusing slightly my status **as an official representative of the Federal Reserve**. I would like to say to Milton [Friedman] and Anna [Schwartz]: **You’re right, we did it**. We’re very sorry. But thanks to you, we won’t do it again.” [emphasis added]*

In other words, Bernanke admitted that the central bankers were responsible for the Great Depression. It does beg the question, though, as to [how many deaths resulting from the Great Depression](#) is the Federal Reserve responsible for? Whatever becomes revealed by statisticians, this much is certain – the Great Depression was used as the justification for social insurance.

Once the [Social Security Act](#) was signed into law by then-President [Franklin Roosevelt](#) in 1935, [Social Security numbers](#) (SSNs) were foisted upon Americans incrementally over time, originally as a tax accounting tool, to be used exclusively for accountability purposes; namely, for calculating each “contribution” into the [Social Security Trust Funds](#) through payroll taxes. Despite the fact that SSNs were never meant to be used for identity verification, they are now commonly required for various functions, especially in the application for licenses **unrelated** to taxation or anything else of a financial nature. In short, the Hegelian Dialectic formula has been repeated multiple times by authoritarians in order to establish a *de facto* national identification tracking number **without** Congress officially doing so through its statutory authority, as delegated by the 1787 Constitution; this was accomplished by disingenuous advocacy that said that the answer to the evils of central banking lay in empowering [administrative agencies](#) to determine welfare handouts by bureaucratic diktat.

Constitutional Avoidance, Statutory Legalities, & Federalist Posturing

Constitutionally, does the federal government retain the power to impose social insurance upon the American citizenry? Both the [Preamble](#) and the Taxing & Spending Clause ([Art. I § 8 cl. 1](#)) have similar **general welfare** provisions, which say, respectively, that:

“We the People of the United States, in Order to form a more perfect Union...provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity...”

“The Congress shall have Power...To pay the Debts and provide for the common Defence and general Welfare of the United States...”

As much can be assumed that “provide for the common defense” might be nothing more than a male citizen’s obligation to submit to the military draft by way of its statutory [compulsory registration law](#), yet, promoting and/or providing for the “general welfare” is more of a challenge to determine its meaning, especially considering that the very word, “welfare,” itself has been [verbicided](#). Needless to say, it is essential to understand what the Framers had to say as to their original intent in crafting that phrasing into the federal Constitution.

[James Madison](#), the Father of the Constitution, had a rather limited view of the general welfare's composition. As Madison wrote in [Federalist Paper #41](#):

"Some, who have not denied the necessity of the power of taxation, have grounded a very fierce attack against the Constitution, on the language in which it is defined... No stronger proof could be given of the distress under which these writers labor for objections, than their stooping to such a misconstruction. Had no other enumeration or definition of the powers of the Congress been found in the Constitution...the authors of the objection might have had some color for it; though it would have been difficult to find a reason for so awkward a form of describing an authority to legislate in all possible cases. A power to destroy the freedom of the press, the [trial by jury](#), or even to regulate the course of descents, or the forms of conveyances, must be very singularly expressed by the terms 'to raise money for the general welfare.'"

In other words, the concept of the **general welfare** cannot be used to circumvent the enumerated powers delegated to the federal government by its own Constitution; otherwise, it wouldn't be a very "[limited](#)" government, would it? From what can be construed, other references within *The Federalist Papers* strongly imply that the general welfare is tightly related to the common defense; specifically, that (according to [Webster's 1828 Dictionary](#)) the "exemption from any unusual evil or calamity; the enjoyment of peace and prosperity, or the normal blessings of society and civil government" is only possible due to military defense of the national realm, especially its borders, as was the case during the [War of 1812](#).

Perhaps a further examination of the relationship between taxation and the public (re: national) debt could illuminate the true nature of the general welfare itself. As Alexander Hamilton wrote in *Federalist Paper #30*:

"Money is with propriety considered as the vital principle of the body politic; as that which sustains its life and motion, and enables it to perform its most essential functions. A complete power, therefore, to procure a regular and adequate supply of revenue, as far as the resources of the community will permit, may be regarded as an indispensable ingredient in every constitution."

Hamilton stressed the necessity for tax revenue as the lifeblood for the execution of other government powers. Interestingly enough, Cincinnatus wrote in [Anti-Federalist Paper #12](#):

"If the new government raises this sum in species on the people, it will certainly support public credit, but it will overwhelm the people. It will give immense fortunes to the

speculators; but it will grind the poor to dust. Besides, the present government is not redeeming the principal of the domestic debt by the sale of western lands...[p]erhaps it will be found, that the supposed want of power in Congress to levy taxes is, at present a veil happily thrown over the inability of the people; and that the large powers given to the new government will, to every one, expose the nakedness of our land. Certain it is, that if the expectations which are grafted on the gift of those [plenary powers](#), are not answered, our credit will be irretrievably ruined."

In other words, [the power to tax is the power to destroy](#). Of course, this begs the question as to whether the "complete power" of taxation would inevitably ruin the credit of the United States, pursuant to the Borrowing Clause ([Art. I § 8 cl. 2](#))? It would seem as if the modern history of repetitive increases in the [debt ceiling](#) have answered this question for us.

Statutorily, is it possible for the federal Congress to impose social insurance as an exercise of its enumerated powers? Although the [Social Security Administration](#) (SSA) was established by the [Social Security Act of 1935](#), the payroll taxes that were intended to fund the Old-Age, Survivors, and Disability Insurance (OASDI) "trust funds" weren't collected until the passage of the [Federal Insurance Contributions Act \(FICA\) of 1937](#). Once this happened, the FICA payroll taxes were allocated towards funding the OASDI, from which the Social Security checks were issued to the qualified recipients; interestingly, § 210(c) of the original 1935 act said that the only "qualified individuals" were those who were 65 years old and had earned more than \$2,000 beginning in 1937 ([survivors and disabled benefits weren't added until 1939 and 1954](#), respectively).

Judicially, are the FICA payroll taxes and the OASDI payouts a constitutional exercise of both the taxation and general welfare clauses? Such a pivotal question strikes at the very legitimacy of the social insurance mechanism that is [Social Security](#) itself. Judge Roberts wrote the United States Supreme Court's opinion in *United States v. Butler*, [297 U.S. 1](#) (1936):

*"Since the foundation of the nation, sharp differences of opinion have persisted as to the true interpretation of the [general welfare] phrase. Madison asserted it amounted to no more than a reference to the other powers enumerated in the subsequent clauses of the same section; that, as the United States is a government of limited and enumerated powers, the grant of power to tax and spend for the general national welfare must be confined to the enumerated legislative fields committed to the Congress. In this view, the phrase is mere tautology, for taxation and appropriation are or may be necessary incidents of the exercise of any of the enumerated legislative powers. Hamilton, on the other hand, maintained the clause confers a power separate and distinct from those later enumerated is not restricted in meaning by the grant of them, and Congress subsequently has a substantive power to tax and appropriate, limited only by the requirement that it shall be exercised to provide for the general welfare of the United States. **Each contention has had the support of those who views are entitled to weight.** This court has noticed the question, but has never found it necessary to decide which is the true construction. Mr. Justice Story, in his Commentaries, espouses the Hamiltonian position. **We shall not review the writings of public men and commentators or discuss the legislative practice. Study of all these leads us to conclude that the reading advocated by Mr.***

Justice Story is the correct one. While, therefore, the power to tax is not unlimited, its confines are set in the clause which confers it, and not in those of section 8 which bestow and define the legislative powers of the Congress. It results that the power of Congress to authorize expenditure of public moneys for public purposes is not limited by the direct grants of legislative power found in the Constitution.” [emphasis added]

Obviously, Roberts is referring to *Federalist Paper #41*, but [Hamilton did not argue in favor of a broader interpretation of the general welfare until after the federal Constitution](#) had been ratified. This interpretation of the general welfare becomes significant in Judge Cardozo's written opinion in *Helvering v. Davis*, [301 U.S. 619](#) (1937):

“There have been great statesmen in our history who have stood for other views. We will not resurrect the contest. It is now settled by decision [in the Butler case]. The conception of the spending power advocated by Hamilton and strongly reinforced by Story has prevailed over that of Madison, which has not been lacking in adherents.”

So, Cardozo was simply reminding everyone, via [stare decisis](#), what Roberts had written a year earlier regarding which interpretation the Court was going to use from here on out. Cardozo then gives some uniquely revealing details:

*“The purge of nation-wide calamity that began in 1929 has taught us many lessons. Not the least is the solidarity of interests that may once have seemed to be divided...**Congress did not improvise a judgment when it found that the award of old age benefits would be conducive to the general welfare.** The President's Committee on Economic Security made an investigation and report, aided by a research staff of Government officers and employees, and by an Advisory Council and seven other advisory groups. Extensive hearings followed before the House Committee on Ways and Means, and the Senate Committee on Finance. **A great mass of evidence was brought together supporting the policy which finds expression in the act...The problem is plainly national in area and dimensions.** Moreover, laws of the separate states cannot deal with it effectively...**States and local governments are often lacking in the resources that are necessary to finance an adequate program of security for the aged.**” [emphasis added]*

Ah-ha! So, here is the justification for Social Security as the “solution” to the Great Depression – because the Federal Reserve caused the Crash of 1929, therefore the U.S. Congress must impose social insurance, as a bulwark against financial crises, in order to provide for the retirement of the elderly? Further elaborating on the structure of Social Security is Judge Harlan writing in *Flaming v. Nestor*, [363](#)

*“The Social Security system may be accurately described as a form of a social insurance, enacted to Congress’ power to ‘spend money in aid of the general welfare,’ whereby persons gainfully employed, and those who employ them, are taxed to permit the payment of benefits to the retired and disabled, and their dependents. Plainly the expectation is that many members of the present productive work force will in turn become beneficiaries rather than supporters of the program. But **each worker’s benefits**, though flowing from the contributions he made to the national economy when actively employed, **are not dependent on the degree to which he was called upon to support the system by taxation. It is apparent that the noncontractual interest of an employee covered by the Act cannot be soundly analogized to that of the holder of an annuity, whose right to benefits is bottomed on his contractual premium payments.**” [emphasis added]*

Simply put, **there is no contract** between taxpayers and the SSA in terms of receiving those coveted Social Security “benefits” once full retirement age has been met. Harlan elaborated on this revealing situation:

*“Particularly when we deal with a withholding of a noncontractual benefit under a social welfare program such as this, we must recognize that **the Due Process Clause can be thought to interpose a bar only if the statute manifests a patently arbitrary classification, utterly lacking in rational justification. Such is not the case here.**” [emphasis added]*

Given that the due process clause (would that be from the Fifth or Fourteenth Amendment?) is *not* arbitrarily classifying Social Security recipients, then the **general rule** of there being **no contract** between the SSA and taxpayers is what’s happening here. In other words, baby boomers and others who insist that they are “owed” Social Security checks because they “paid into the system” are woefully ignorant of the government’s interpretation of its own laws. Needless to say, because **there is no contract**, Social Security recipients are not “owed” a damn thing; Harlan goes on to describe in *Flaming* how Congress can change the schedule of “benefits” entirely at its own discretion.

In a rather uniquely illuminating piece of government literature, the SSA’s Office of Legislative and Regulatory Policy issued [a Social Security Bulletin in January of 1987](#) about the very constitutionality of Social Security itself. According to the bulletin’s author, Eduard Lopez:

“Of course, the Court’s decisions in the social security cases, represented a significant

constitutional development in establishing the breadth of Congress' powers to tax and spend for the general welfare. The decisions not only cleared the way for other general welfare programs, but more fundamentally provided the Federal Government with the substantive power and institutional flexibility to respond to the changing needs of the Nation."

Lopez, much like Judge Roberts in the *Butler* case, compared and contrasted the two Madisonian and Hamiltonian views of federalism, but this time regarding the Supremacy Clause ([Art. IV cl. 2](#)) and the [Tenth Amendment](#). Briefly put, Lopez said that the Hamiltonian view is that of "subordinate States" and the Madisonian view of the several state governments being "coequal sovereigns" with the national government; Lopez goes on to mention that "coequal sovereigns" was the original view of the U.S. Supreme Court from the mid-19th century to 1937, and that the "subordinate States" view took over since the late 1930s. [Court-packing](#), much?

Considering all the legalities at play, **what is the constitutionality of Social Security?** You must keep in mind that in *Helvering*, Cardozo mentioned that only the FICA payroll taxes are constitutional, pursuant to the Taxing & Spending Clause, yet the Court, by their adherence to the [Ashwander rules](#), totally dodged the question of the OASDI payouts; the closest answer to the latter issue was the lack of a contract mentioned by Harlan in *Flaming*. What this demonstrates, if anything, is that the Court's use of both [judicial review](#) (that is, ruling on the constitutionality of the matter brought before them for adjudication) and [constitutional avoidance](#) are often practiced whenever they want to either preserve or increase the power of the federal government, but seldom to limit or reduce it.

Financing Socialized Retirement

Economically, what are the costs of Social Security? [According to the Tax Policy Center](#), the federal payroll tax rate has increased from less than 3% to more than 12% over 70 years; [the Joint Committee on Taxation](#) found that the federal payroll tax burden has increased from approximately 10% to an estimated 40% over 50 years. Considering the enlarging tax revenues, you'd expect those subsidized "benefits" to increase, but such would not be an entirely accurate financial portrait.

[Government shutdowns](#), [credit-rating downgrades](#), and [unfunded liabilities](#) do not bode well for the financial solvency of the U.S. federal government. The [2011 debt-ceiling crisis](#) precipitated the credit downgrade of the national government from AAA to AA+, yet the lingering budgetary issues went unresolved, eventually culminating in the [2013 debt-ceiling crisis](#), which itself resulted in [a government shutdown later that year](#) (such a shutdown has not occurred [since the mid-1990s](#)). According to the White House's [Office of Management and Budget](#) (OMB), gross national debt has increased from less than \$1 *trillion* to more than \$14 *trillion* over 70 years.

Discovering the proportion of Social Security's unfunded liabilities relative to the gross national debt is imperative for understanding the true financial costs of social insurance. This past December 12th, [the gross national debt stood at \\$18.7 trillion](#); for the past six years, [according to the annual reports from the OASDI's board of trustees](#), Social Security's unfunded liabilities through the 2080s (on a annually shifting 75-year time frame) have *increased* from \$5.4 trillion in 2010 to \$10.7 trillion this year. So, not only are Social Security's unfunded liabilities compose a **5/9ths majority** of the gross national debt **just this year**, but they are also the **fastest growing** portion of it, considering its growth relative to the entirety of the gross national debt.

Because of these unfunded liabilities, the OASDI is paying out more than is being replenished by FICA taxes. [Dave Duffy wrote in 2001](#):

“There is no trust fund that holds social security money. The trust fund holds government bonds, which is a type of IOU, which will be paid off by raising taxes on future generations, or by simply drastically cutting back the benefits paid to future retirees. Although the government’s income from social security taxes is currently greater than the outgo to today’s recipients, the extra cash is simply put into the government’s general fund and spent. Nothing but another IOU is put into the social security trust fund.”

Duffy went onto say that Social Security was **underfunded** by about \$20 trillion, but isn’t this just an exaggeration? [According to the Congressional Budget Office \(CBO\) in 2013](#), **Social Security will become exhausted by 2033**. Obviously, the big question once Social Security becomes “officially” insolvent is, what’s next? [According to the Congressional Research Service \(CRS\) in 2014](#):

“The Social Security Act does not state what would happen to the payment of benefits scheduled under current law in the event of a Social Security trust fund exhaustion... [w]hen current revenues are not sufficient to pay benefits, however, the U.S. government must raise the funds necessary to honor the redemption of U.S. government obligations held by the Social Security trust fund as they are needed to pay benefits. If there are no surplus governmental receipts, the U.S. government may raise the necessary funds by increasing taxes and other income, reducing other spending, borrowing from the public (i.e., replacing bonds held by the trust fund with bonds held by the public), or some combination of these measures.”

This would seem to answer the question of what happens post-bankruptcy, yet, why does CRS implicitly appear to contradict Duffy regarding the very existence of the Social Security “trust funds” themselves? [As “Loren” from SSA said just this past month](#):

*“It is important to understand that the money you pay in Social Security taxes is not held in a personal account for you to use when you get a Social Security payment. Your taxes are used **right now** to pay people who are currently getting Social Security payments. In turn, your future Social Security benefits will be paid by future workers.”*

Interestingly, [Milton Friedman said the exact same thing over three decades ago](#); namely, that **workers**

subsidize retirees. So, at most, the “trust funds” are really nothing more than an accounting tool to track “intragovernmental debt,” and this is further confirmed by the 2014 CRS report. Put simply, because SSA is unable to maintain an equilibrium between FICA taxes and OASDI payouts, the next few generations are being saddled with unpayable debts, and this will likely result in either a [currency war](#) or [sovereign default](#).

Constitutionality may have indeed legitimized socialism, yet the laws of economics do not reward central planning, as can be evidenced by the growing federal payroll tax burden, unfunded liabilities, and ever-increasing debt ceiling. Taxation has truly ruined the credit of the United States, which Cincinnatus warned about in *Anti-Federalist Paper #12*, and this is evidenced by the federal government’s credit-rating downgrade. However, this is not a [doom porn scenario](#) by any means, particularly considering that if the current downward class migration degenerated further into a hyperinflationary depression, it would not result in a post-apocalyptic dystopia because this would interfere with the “business as usual” of fractional reserve lending that enables the State to parasitically feed off of the Market; in other words, a total socio-economic collapse would be to kill the goose who laid the golden egg.

The only real pertinent question left at this point is, how many years of Social Security subsidies can retirees expect to collect on? [According to the 2015 OASDI Trustees Report](#), the total benefit payments were \$848.5 *billion*, and these payments were made out to about 59 *million* people; this would mean that the average 2015 Social Security subsidy per recipient was \$14,381 (this is hovering around last year’s [poverty threshold](#)). If you consider the [World Health Organization \(WHO\) data on life expectancy](#), then the average male life expectancy from birth in America is 76 years, as opposed to females at 81 years. Assuming that the retirement age is not raised by remaining at 67 years, then the average total retirement subsidies per citizen can be calculated using the following formula:

(Average life expectancy – retirement age) X the average Social Security subsidy per recipient = average total retirement subsidies per citizen

Mathematically, plugging in the numbers for males and females, respectively, yields the following calculations:

$$(76 - 67) \times \$14,381 = \$129,375$$

$$(81 - 67) \times \$14,381 = \$201,250$$

This means that, on average, female Social Security retirees are paid \$71,875 *more* during their golden years than their male counterparts, based solely on their longer life expectancy. How is this indicative of the “[equality](#)” Elizabeth Warren demanded as a “progressive” commandment? [Gender gap](#), much?

Social Security is nothing more than socialized retirement, and an unequal one at that, especially considering how the FICA payroll tax is **regressive** due to [its tax cap at \\$118,500](#) per year. To briefly review, because of the 1907 panic caused by the Treasury department’s inflation, central banking was

reintroduced, which about two decades later caused the Great Depression, thereby providing a convenient pretext for the federal government to impose social insurance. This, in turn, led to the CBO's projection of the OASDI's exhaustion by 2033, which just might lead to a sovereign default or currency war. Simplifying this further using the Hegelian Dialectic, the recurring historical patterns appear to be as such:

- **Round #1:** *Inflation (the problem) → bank runs/panic (the reaction) → central banking (the “solution”)*
- **Round #2:** *Central banking (the problem) → Great Depression (the reaction) → social insurance (the “solution”)*
- **Round #3:** *Social Security (the problem) → debt ceiling increases/credit-rating downgrade/government shutdowns (the reaction) → currency war and/or sovereign default (the “solutions”)*

Needless to say, social insurance is a total lie, not just because of its financial insolvency, but also because it is constitutionally funded by payroll taxation, as well as the fact there is no contractual right to be paid its subsidized “benefits,” as Judge Harlan mentioned in the 1960 *Flaming* case. Upon a comprehensive review of Social Security, this is but just one story of the collusion between lawyers and bankers in their unholy mission to utterly destroy American liberty.

The Despicable Evil of Social Security Numbers

Last June, I was asked by an insurance agent for my SSN just to get a renter's insurance *quote*; fortunately when I refused, an alternative was used so I could discover that there was an opportunity for me to lower my annual bill by \$20. Earlier this month, [Eric Peters was asked by a police officer for his SSN during a traffic stop](#), which he promptly gave. Identity theft has increased from [11.7 million](#) to [17.6 million](#) between 2010 – 2014; thankfully, the financial loss during this same period decreased from \$17 billion to \$15.4 billion (although there was [an uptick in 2012 of \\$24.7 billion](#)).

Charles Mullen, the Associate Commissioner at the SSA's Office of Public Inquiries, [wrote a reply to Scott McDonald on March 18th of 1998](#). Mullen revealed that:

“The Social Security Act does not require a person to have a Social Security number (SSN) to live and work in the United States, nor does it require an SSN simply for the purpose of having one. However, if someone works without an SSN, we cannot properly credit the earnings for the work performed.”

This supports what [Claire Wolfe mentioned in 2003](#), and it does jive with the rest of the SSA literature that says the SSN is used as a way to determine eligibility for retirement subsidies. However, as with any “good” government “program,” exceptions to the general rule contain the most inconvenient surprises. Mullen continues:

*“The Privacy Act regulates the use of SSNs by government agencies. **They may require an SSN only if a law or regulation either orders or authorizes them to do so. Agencies are required to disclose the authorizing law or regulation.** If the request has no legal basis, the person may refuse to provide the number and still receive the agency’s services. However, **the law does not apply to private sector organizations. Such an organization can refuse its services to anyone who does not provide the number on request.**” [emphasis added]*

Obviously, the scope of said laws and “regulations” can be so broad as to render the general rule of no compulsory numbering a moot point, but is that the case here? Mullen provides two such examples, namely, [26 USC § 6109\(a\)](#) and [26 CFR § 301.6109-1\(d\)](#), which say, respectively, that:

*“When required by regulations prescribed by the Secretary: Any person required under the authority of this title to make a return, statement or other document such identifying number as may be prescribed for securing proper identification of such person...for purposes of [this paragraph], the identifying number of an individual (or his estate) shall be such individual’s **social security account number.**” [emphasis added]*

*“Any individual required to furnish a **social security number** pursuant to paragraph (b) of this section shall apply for one, if he has not done so previously, in Form SS-5, which may be obtained from any Social Security Administration or Internal Revenue Service office. He shall make such application far enough in advance of the first required use of such number to permit issuance of the number in time for compliance with such requirement. The form, together with any supplementary statement, shall be prepared and filed in accordance with the form, instructions, and regulations applicable thereto, and shall set forth fully and clearly the data therein called for. Individuals who are ineligible for or do not wish to participate in the benefits of the social security program shall nevertheless obtain a **social security number** if they are required to furnish such a number pursuant to paragraph (b) of this section.” [emphasis added]*

Well, geez, I wonder which individuals are required to cough up an SSN? 26 CFR § 301.6109-1(b) says:

*“Every U.S. person who makes under this title a return, statement, or other document must furnish its own taxpayer identifying number as required by the forms and the accompanying instructions. A U.S. person whose number must be included on a document filed by another person must give the taxpayer identifying number so required to the other person on request. For penalties for failure to supply taxpayer identifying numbers, see sections 6721 through 6724. For provisions dealing specifically with the duty of employees with respect to their **social security numbers**, see § 31.6011(b)-2 (a) and (b) of this chapter (Employment Tax Regulations)...” [emphasis added]*

These penalties range anywhere from \$50 to \$100,000 for failures regarding payee statements or “specified information reporting requirements,” up to a further maximum of \$250,000 for failures regarding information returns; the Employment Tax Regulations demand new employees to furnish an SSN to their employers, or otherwise immediately acquire one through filing an SS-5 form to SSA, in order to be in compliance with being subjected to taxes as imposed by FICA. In other words, if you are an employee working for wages, you must submit an SSN to your employer so you can pay FICA taxes.

Although it is true what Mullen said, the devil is in the details, particularly the *broad* application of the exceptions to the general rule. According to this year’s [SSA Pub #05-10023](#):

“Getting a Social Security number for your newborn is voluntary.”

Naturally, this is consistent with Mullen, for infant Americans (by and large) are not employees working for wages, and thus do not incur a federal income tax liability. Surely it is understandable why [Claire Wolfe earlier this year began using her SSN again](#), because quite a bit of the American workforce is composed of employees working for wages. The fact of the matter is that because of the way in which most Americans earn their livelihoods, their SSNs are initially used for tax accounting purposes, and then oh-so-conveniently morphed into a nearly universal tool for identity verification as the *de facto* national ID number; in this context, SSA’s assurances over the course of 17 years that getting an SSN is voluntary provides little comfort, simply because the exceptions to the rule are broader than the rule itself.

Mullen’s letter also mentioned that the [Privacy Act of 1974](#) does not apply to private sector organizations, and thus, they presumably reserve the right to refuse service to any customer who doesn’t provide their SSN on request; this is reinforced by [Dorcas Hardy’s 1986 letter to Rodney Rickman](#), which said that SSA does not have the authority to require employers to make employment decisions based on whether the potential employee refused to disclose his SSN, as this is a matter exclusively between the job-seeker and the employer. Given that private businesses enjoy [the right to refuse service](#), then do government regulations, such as “[know your customer](#)” laws, infringe on that right? [According to the Government Accountability Office \(GAO\)’s 2004 report on SSNs](#):

*“Large information resellers said that they generally use the SSN as an identity verification tool. Some of these entities have incorporated SSNs into their information technology, while others have incorporated SSNs into their client’s databases used for identity verification. For example, one large information reseller that specializes in information technology solutions has developed a customer verification data model that aids financial institutions in **their compliance with some federal laws regarding ‘know your customer.’** According to this company’s information, the data model compares information provided by the applicant, such as name, address, and SSN, with the data they already have in their databases, which is composed of multiple public and private sources.” [emphasis added]*

Obviously, the degree of voluntariness regarding the use of SSNs begins to slide headlong on the [slippery slope](#) of institutionalized coercion. It's a little hard to say with a straight face that getting a SSN is voluntary, but then create these hugely gaping legal exceptions, such as compliance with administrative business regulations or the statutory tax code. GAO's report also says:

"The Social Security Act of 1935 authorized the Social Security Administration (SSA) to establish a record-keeping system to help manage the Social Security program, and this resulted in the creation of the SSN...SSA estimates that approximately 277 million individuals currently have SSNs. Because of the number's uniqueness and broad applicability, the SSN has become the identifier of choice for government agencies and private businesses, and thus it is used for a myriad of non-Social Security purposes."

Since more than three-fourths of the domestic American population has SSNs, this means that a [captive market](#) for potential identity theft has been generated thanks to the lackadaisical federal bureaucracy. It could be said that, in addition to the three aforementioned rounds of the Hegelian Dialectic, there is yet another round, which is:

- **Round #4:** *Identity theft (the problem) → demand for "[consumer protections](#)" (the reaction) → SSNs being used for identity verification (the "solution")*

This is something that you must contend with directly, for unlike collective phenomenon like sovereign defaults, currency wars, or downward class migration, identity theft is committed primarily against individuals; this suggests that the responsibility for preventing and otherwise dealing with identity theft lies with individuals, as well. You are not able to influence government policy about social insurance through "[reform](#)," but what you can do is make yourself a [hard target](#) against identity thieves.

Some have claimed over the years that rescission of one's SSN is possible, but that [SSA will obstruct you at every turn](#); the basis for this claim lies in Form SS-521, [Request for Withdrawal of Application](#). However, the "application" in question is none other than Form SS-5, [Application for Request of Social Security Card](#). In other words, if a parent has submitted the SS-5 for their infant in order to get a tax deduction, and then changes his mind for whatever reason, then he'll have to submit the SS-521. Aside from circumstances like that, where the SSN was applied for, but not used, then generally speaking, **there is no such thing as rescission of an SSN**. Once the SSN is received and used, then it is simply too late to "request a withdrawal," mainly because by then, the application has been received and accepted by SSA, as evidenced by their issuance of a new Social Security card. In this respect, it would be accurate to say that SSNs are much like quicksand, in that you can avoid them, but once you're in, it becomes increasingly difficult to escape the longer you're in it; because of this, I think it is wiser to examine other options for dealing with your SSN rather than place blind faith in any "[sovereign citizen](#)" type of baseless assertions.

To reiterate, Mullen's 1998 letter mentioned how the Privacy Act only limits the government in requiring an SSN from you, but that the statute does *not* limit private companies at all. This would mean that my own situation could have turned out very differently where I could have not received an insurance quote because I had refused to give my SSN, because I was dealing with a for-profit corporation, not a

government agency. By contrast, though, this does beg the question as to whether the police officer who asked Eric Peters for his SSN during a traffic stop violated the Privacy Act? According to [5 USC § 522a\(g\)\(4\)](#), it says:

*“In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was **intentional** or **willful**, the United States shall be liable to the individual in an amount equal to the sum of – (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and (B) the costs of the action together with reasonable attorney fees as determined by the court.”*
[emphasis added]

Huh, I wonder what circumstances and jurisdiction are enumerated in 5 USC § 522a(g)(1)(C) and (D):

“Whenever any agency...fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.”

This is rather intriguing, for it suggests that Peters *might* have standing to sue the police *if* he could demonstrate **intentional willfulness** on the part of the officer (of course, the jurisdictional matter of the [incorporation doctrine](#) would also be at issue, given that such a lawsuit under the Privacy Act would have to be done in federal district court against who would presumably be an agent of one of the several *state* governments). Perhaps [42 USC § 405\(c\)\(2\)\(C\)\(i\)](#) can illuminate the situation better:

*“It is the policy of the United States that any State (or political subdivision thereof) may, in the **administration** of any tax, general public assistance, **driver’s license, or motor vehicle registration law within its jurisdiction**, utilize the social security account numbers issued by the Commissioner of Social Security for the purpose of establishing the identification of individuals affected by such law, **and may require any individual** who is or appears to be so **affected to furnish to such State** (or political subdivision thereof) or any agency thereof having **administrative responsibility** for the law involved, **the social***

security account number (or numbers, if he has more than one such number) issued to him by the Commissioner of Social Security.” [emphasis added]

Understand all that? Put simply, the question here is, did the officer have the legal “authority” to **administer** driver licensure or vehicle registration at the side of the road? If so, then that is the end of the case, for then Peters was obligated to give his SSN, as he did; if not, then Peters would be in a position to use the civil remedies under the Privacy Act to sue the officer (14th Amendment issues, notwithstanding). Obviously, I am very skeptical whenever anyone recommends [suing the government](#) for anything, especially considering all the [patriot mythology](#) floating around the Internet.

Another set of approaches towards safeguarding your SSN from identity thieves and other miscreants, as some have recommended, is to [go on a paper trip](#), or [civilly disobey](#) federal law by giving patently false SSNs whenever you are asked for one. Due to the complexity of the former, I prefer to forego that here, other than to reiterate in previous book reports the fact that paper-tripping is simply nothing more than the **legal** exploitation of government loopholes; also, the civil disobedience avenue was alluded to earlier in reference to the penalties enumerated in [26 CFR §§ 301.6721-1\(a\), 301.6722-1\(a\), and 301.6723-1\(a\)](#).

Yet another possibility is that you could engage in what might be termed, “libertarian pyrotechnics,” regarding your Social Security card. [Russell Kanning and Kat Dillion burned their Social Security cards outside an SSA field office back in 2006](#) and [Mike Gogulski did the same to his in 2009](#). I guess as long as you resolve to never use either the card or the SSN itself ever again, this is probably the most legally hassle-free way to rid yourself of it, but as [Claire Wolfe accurately pointed out](#), this is easier said than done, unless [you have made arrangements for your change in lifestyle ahead of time](#).

Lessons Learned?

Social Security is little else than an unsustainable [perverse subsidy](#). Anyone who insists otherwise is living in denial. Four rounds of the Hegelian Dialectic have brought Americans under the heel of central bankers and the federal bureaucracy. If anything is to be learned from this rather sordid history, it is that no one can [centrally plan](#) anyone else’s retirement. Austrian economist Ludwig von Mises remarked in his 1949 [Human Action](#) that:

*“The problems involved are not of a praxeological character, and economics is not called upon to provide the best possible solution for them. They concern pathology and psychology. They refer to the biological fact that the fear of penury and of the degrading consequences of being supported by charity are important factors in the preservation of man’s physiological equilibrium. They impel a man to keep fit, to avoid sickness and accidents, and to recover as soon as possible from injuries suffered. The experiences of the **social security** system, especially that of the oldest scheme, the German, has clearly shown **the undesirable effects resulting from the elimination of these incentives**. No civilized community has callously allowed the incapacitated to perish. But the substitution of a legally enforceable claim to support or sustenance for charitable relief does not seem to agree with human nature as it is. Not metaphysical prepossessions, but considerations of practical expedience make it inadvisable to promulgate an actionable right to sustenance.”*

Passing off coercion as if it were charity is, perhaps, the most despicable thing [progressive socialists](#) have done (short of causing a sovereign default with all their [welfare entitlement spending](#), of course). [As I've mentioned before](#), inflation destroys the value of the capital saved from the past, taxation robs from the fruit of one's labor in the present, and borrowing enables deficit spending whose bill is shouldered upon the backs of the unborn. All three of these control mechanisms are present in the story of Social Security, which is really just the American version of what the German [NSDAP's](#) party platform demanded for "[a generous increase in old-age pensions](#)." National socialism, much?

The epic fail of social insurance also begs the question as to the government's enabling of identity theft. Not only are the implications of parents applying for SSNs (so they use their infants for tax deductions) quite profound, but also the fact that **identity verification is indispensable for government licensure**. Acquiring even the more purely elective marriage or ham radio license without an SSN might be biting off more than some can chew. Until the government is abolished, jealously guarding your SSN is the only real mitigation to take for the time being in terms of direct action on this issue (other than [never taking a Social Security "benefit" check](#) as an OASDI payout). [Keeping your own counsel](#) has been suggested in a myriad of ways; Robert Smith listed the following recommendations in his book, [Our Vanishing Privacy](#):

- Don't put your number on an employment application; wait until you are hired.
- Do provide a Social Security number to an agency that will be paying you a salary or interest or dividends, charging you interest, or maintaining a checking or savings account for you.
- Do remember that state motor vehicle departments, tax departments, and welfare departments are authorized to demand an SSN. Otherwise, do not provide a Social Security number to any government agency unless it provides you with its authority to do so and its uses for the number.
- Try not to provide your number to the motor vehicle office unless it insists on it; in many states the motor vehicles department will waive its original demand for a SSN. Even if you must provide it, try to avoid having your SSN used as your driver's license number and printed on your license.
- Use caution when you are asked for your Social Security number by a retail store, a utility company, a private college, an insurance company, a credit-card company, or other private business. No law says you have to give it; no law says the company has to do business with you. Try providing only the last four digits. Or provide the number with a statement asking that it not be disclosed further. Ask that the number not appear on mailing labels.
- Don't provide your SSN when you cash a check or pay by credit card. Make clear why you are objecting.
- Don't provide your Social Security number over the telephone.
- Avoid enumerating your child at an early age. Most requests for SSNs by [public school systems](#) are not enforceable.
- Remember that federal law requires a Social Security number on your tax return for any child two years or older claimed as a dependent. Federal law requires that a child receiving Aid to Families with Dependent Children (AFDC) have a Social Security number. And some states require *parents'* Social Security numbers on applications for birth certificates (but not on the actual certificate itself). If you feel strongly about not enumerating your children, you can waive your claim to a tax deduction. Or, like Suzanne Watson in California, you can battle the IRS and perhaps win.

Aside from these guidelines, I would also proffer that you all examine Privacy Rights Clearinghouse's Fact Sheet #10, [My Social Security Number – How Secure Is It?](#) for more specific ideas on how to safeguard your SSN from identity thieves.

How might it be possible to avoid the temptations of Social Security's OASDI payouts as a retiree? **The answer to social insurance is financial independence.** Paying FICA taxes *hurts* you, and noticeably more so if you are male than female; because FICA is a *regressive* tax, then the payroll tax cap might actually help you *if* you can earn more money ([income taxes](#), notwithstanding). [Financially independent early retirement](#) does not violate self-ownership, like how Social Security does. Whether it be by way of freelancing, intensive saving, passive/residual income, and/or selling a profitable entrepreneurial venture, these are *voluntary* ways of providing for your livelihood, and are a much better financial safety net for your old age than some government program that can unilaterally change the terms of its "benefit" payments any time it wants.

I honestly don't know to what degree modern Americans are willing to sacrifice the conveniences of the present for the liberty of future posterity. Thomas Jefferson, I think, got it right when [he told Antoine Louis Claude Destutt de Tracy in 1820](#):

"It is incumbent on every generation to pay its own debts as it goes. A principle which if acted on would save one-half the wars of the world."

Unfortunately, as mentioned earlier, workers subsidize retirees through FICA taxes, so this is obviously in contravention to what Mr. Jefferson admonished the French over. What I appreciate about his observation is the historical link between debt and war; whether it be [socialized war debts](#) or socialized retirement, Leviathan has a nasty habit of coercing its victims to pay for things they either don't want, or think is unethical. In summation, I think [Stefan Molyneux best describes](#) my innermost feelings towards [the State](#):

*"Fuck the stupid teachers, fuck the bullshit unions, fuck the debt, fuck the Fed! **Fuck it all!** That's why you get out of bed in the morning, to say, fuck evil!"*

Do You Have the “Right” to be Forgotten?

www.thelastbastille.com/2016/05/23/do-you-have-the-right-to-be-forgotten/

“In the walls of the cubicle there were three orifices. To the right of the speakwrite, a small pneumatic tube for written messages, to the left, a larger one for newspapers; and in the side wall, within easy reach of Winston’s arm, a large oblong slit protected by a wire grating. This last was for the disposal of waste paper. Similar slits existed in thousands or tens of thousands throughout the building, not only in every room but at short intervals in every corridor. For some reason they were nicknamed memory holes. When one knew that any document was due for destruction, or even when one saw a scrap of waste paper lying about, it was an automatic action to life the flap of the nearest memory hole and drop it in, whereupon it would be whirled away on a current of warm air to the enormous furnaces which were hidden somewhere in the recesses of the building.”

– George Orwell’s [1984](#)



There has always existed a natural tension between the free press and individual privacy. Back in 1995, [Dr. Gini Scott](#) argued that there ought to be a balance amongst those who cherish the publication of true information on the one hand, but who also value confidential information on the other. As long as individuals appreciate that [whatever is intended to remain private remains as such](#), alongside championing for [the public's insistence on transparency](#), then an understanding can be reached that relies not so much on ridiculous legalistic “balancing” tests, but rather, a [disciplined market](#) sifting of what is private data versus the public’s domain through the [price system](#).

No advocate of liberty can be taken seriously if they tolerate evils that oppress both the free press and individual privacy, such as censorship and indiscriminate surveillance, respectively. The [freedom of the press](#) and the [right to privacy](#) are both libertarian values that respect [negative liberty](#); that is, the absence of coercion. These values seldom conflict with each other unless there is a dispute about whether the information in question was intended or appropriate for dissemination, or not.

In recent years, there has been a marginally successful political movement of sorts, which has argued that people ought to enjoy their “right to be forgotten.” Originally stemming from the modern French concept of *le droit à l’oubli* (the “[right of oblivion](#)”), this idea asserts that individuals deserve to not have their futures dictated by their past actions, especially for those who are convicted felons, have embarrassing youthful indiscretions, or incurred large debts, any of which could disqualify them from meaningfully participating in such actions as successful rehabilitation, gainful employment, or even approval for mortgages. [According to Wikipedia](#), this “right” to be forgotten is distinguished from the right to privacy thusly:

“The right to be forgotten is distinct from the right to privacy, due to the distinction that the right to privacy constitutes information that is not publicly known, whereas the right to be forgotten involves removing information that was publicly known at a certain time and not allowing third parties to access the information.”

In other words, the right to privacy is uniquely focused on keeping private information confidential, whereas the “right” to be forgotten wants public information to be reverted back to being private. What these advocates of the “right” to be forgotten conveniently, well, *forget*, is that privacy is a one-way street; private data can remain as such, or it can “go public” through disclosure, leaking, and whistle-blowing, **but** public information *cannot* become private again retroactively.

Put another way, [once the cat is let out of the bag](#), it stays out; there is no way to [put the genie back in the bottle](#) (not to mix metaphors!).

Yet, it would seem to be the case that the European Union’s judiciary disagrees with libertarianism. In the 2014 [Google Spain v. AEPD & González](#) case, the EU’s Court of Justice ruled that the plaintiff did indeed have a limited “right to be forgotten,” particularly as it applied to his grievance that he deserved to have Google permanently remove the search result indices that revealed he was a credit risk for a mortgage due to a foreclosure from years past. This decision was adjudicated primarily on the basis of [Directive 95/46/EC](#), whose Article 12(b) said that:

*“Member States shall guarantee every data subject the right to obtain from the controller: as appropriate the rectification, **erasure or blocking of data** the processing of which does not comply with the provisions of this Directive, in particular because of the **incomplete or inaccurate nature of the data**...” [emphasis added]*

What is awfully peculiar about the Court’s decision in this case is that González’s bankruptcy and foreclosure was all *true* – none of it was libel or defamation upon his character or reputation. Regardless of the truthfulness of González’s past, the Court explained that:

“According to Mr. Costeja González and the Spanish and Italian Governments, the data subject may

oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy – which encompass the ‘right to be forgotten’ – override the legitimate interests of the operator of the search engine and the general interest in freedom of information.”

So, it would appear that the fix was in to interpret the Directive beyond its enumerated limits regarding the “erasure or blocking of data” when such data is of an “incomplete or inaccurate nature.” It also didn’t matter that this EU court’s own [advocate general was dead set against this proposed “right” to be forgotten](#), for they ignored him anyway. Much like the United States Supreme Court’s “[doctrine of incorporation](#)” via the Fourteenth Amendment, the black robed men can rationalize *anything*, so long as the special interest agenda of the moment is justified as a “fundamental right.”

Predictably, the 2014 *González* case resulted in an ironic demonstration of the [Streisand effect](#) in motion, which you would presume would fully discredit the very foundation undergirding the “right” to be forgotten in the minds of those who originally supported its implementation, but you would be wrong for doing so. An [administrative agency](#) known as the Federal Trade Commission (FTC) is involved in trying to gauge how practical it would be to import this “right” to be forgotten from Europe. [Julie Brill](#), then-FTC Commissioner, [made the following statements](#) a few months after the *González* case:

“The ECJ’s Google decision, in my view, was not about a ‘right to be forgotten.’ Instead, as some commentators on my side of the Atlantic observed, it is about a ‘right of relevancy’ or a ‘right to preserve obscurity.’ The case stems from a Spanish citizen, Mario Costeja González, who complained that searches for his name on Google returned information about attachment proceeds relating to social security debts that he owed.”

During April of 2015, [Brill told the Christian Science Monitor](#) that:

“I think we need to expand obscurity protections here in the US, through enactments of legislation that would require data brokers to provide greater protections to consumers, and through more comprehensive privacy legislation...I am optimistic that we can infuse a workable right of obscurity into our privacy framework here in the United States...However, I don’t believe a broad EU-style right to be forgotten will be included in these discussions, because the further reaches of a broad right to be forgotten modeled on the CJEU’s decision would raise serious questions under the First Amendment here in the US...I have long called for consumers to be given tools to enhance their obscurity in other appropriate circumstances.”

Apparently, just as long as the “right” to be forgotten is semantically relabeled the “right” to obscurity, then I guess

everything's just fine, isn't it? Despite Brill's hesitation about *fully* importing the "right" to be forgotten due to its infringement upon the free press, [a 2014 survey by Software Advice](#) revealed that 61% of Americans favor some version of the "right" to be forgotten as being regrettably necessary, and a whopping 39% who want the European-styled "right" to be forgotten with absolutely no restrictions whatsoever.

Why does there seem to be this callous disregard for the remnants of the free press, particularly the alternative media? Franz Werro elucidated in his [2009 white paper](#) that the key difference may very well lie in dissimilar cultural values on each side of the Atlantic:

"[J.Q.] Whitman explains this disconnect between the two western cultures as it exists today by referring to the differing socio-political contexts in which the two bodies of law developed. In his view, the American law is the product of a tradition wary of centralized power, while European law is heavily influenced by French ideas of aristocratic honor and Germanic ideas of autonomy and self-determination. The American distrust of centralized power, therefore, is embodied by the Fourth Amendment's prohibition against unreasonable searches and seizures, which contemplates the home as the primary defense and the government as the primary enemy of privacy."

This does seem to mesh with much of what [Alexis de Tocqueville had to say regarding the Great Experiment](#). Werro continues:

"One way to look at this divide is in terms of the cultural loci of trust; the Europeans' trust in the government and distrust of the market, while Americans take precisely the opposite view. In general, that is, Americans feel that increasing the flow of information to the government is more likely to result in abuse than tangible benefit and Europeans share a similar skepticism with respect to the market; protecting 'privacy' is the vocabulary of both thus demands a shutting off of the flow of information to the institution that the respective society trusts the least...American faith in the private sector comes through in a general preference for market self-regulation and a cautious yet noticeable subscription to the idea that increasing the availability of consumer information will pay dividends in the form of products more closely tailored to consumer preferences. In this sense, the American system embraces not only a firm belief in a free press, but in free enterprise as well, the first being arguably also an essential tool for the second."

Oh, those pesky Americans with their free markets and Fourth Amendment! How dare they [remain skeptical](#) of [central planning](#) and the [police state](#)! Why, if Americans were more like Europeans, the entire planet would be that much closer to the utopia of authoritarian [global governance](#)! All kidding aside, if Werro is right, then that would explain quite a lot about the "right" to be forgotten, wouldn't it?

Thankfully, there are other scholars who aren't completely blind about the difficult reality it would be to import the "right" to be forgotten to this side of the pond, given the historical value shown to the free press within the [common law](#). Dr. Jasmine McNealy's [2012 white paper](#) admitted that:

“Although EU member states hail the creation of this right to be forgotten as improving individual privacy rights, such a right creates a problem for U.S. online news organizations. Not only does such law come into direct conflict with protections found in the First Amendment, but it also conflicts with traditional privacy jurisprudence, which states that information made public cannot become private again.”

Alessandro Mantelero’s [2013 white paper](#) made the astute observation that:

“In both cases the historical figure of the journalist is absent. The journalist defines the boundaries of the right of oblivion in specific cases, by his professional ability to distinguish between individual acts that are no longer relevant and facts that are still relevant or related to other present events of public interest.”

In a similar vein, Emily Shoor wrote in her [2014 white paper](#) that:

“Consistent respect from journalists and individuals could help ‘construct zones of privacy.’ Furthermore, social norms of usage among users that embody this respect could help strengthen users’ privacy. For example, an overwhelming number of people in Japan use pseudonyms on social networking sites. A survey conducted in Japan noted that 89% of users of social media were reluctant to use their real name publicly on the Internet.”

Despite this concession, Shoor appears to still advocate for the “right” to be forgotten:

*“The Right to Be Forgotten is intended to grant control of one’s personal data back to the individual... [p]rotection against **reputational harm** is important for job hunting, but another benefit of the proposed Regulation is one’s ability to take down content that is not only harmful, but simply undesirable. The Right to Be Forgotten would allow people to delete content they regret posting, not just content causing them harm...[t]he Right to Be Forgotten establishes a **universal right** of privacy for all citizens of the EU, and provides a significant amount of autonomy over one’s online identity and reputation. While this concept receives a significant amount of backlash, **the Right to Be Forgotten is derived from existing European privacy laws**. Privacy is **a fundamental right granted** under the European Convention for Human Rights and has long been honored by various European*

countries...[t]he Right to Be Forgotten allows people to live life without their past interfering with their future.” [emphasis added]

This is one more reason I don’t like “positive” liberty, because there is this assumption that *civil* rights are *granted* to you by an *authority*, usually a government.

Speaking of “positive” liberty, the expectation of an obligation upon someone else to do something for you without compensation is **slavery**, pure and simple. The fundamental problem with the “right” to be forgotten is that it unilaterally imposes an obligation upon individuals to destroy their own records upon arbitrary demand. Market feedback depends upon information being freely available, whether that takes the form of product reviews or credit reports.

What is little understood by authoritarians is that the free press can disincentivize (and even punish) bad behavior through the publication of truthful information about specific individuals and their provable actions, all of which is done peacefully. Any such blacklisting of individuals will be impossible to enforce through [ostracism](#) if this “right” to be forgotten can be exercised on a mere whim. In effect, the “right” to be forgotten strips the [market’s capability of spontaneous order](#) in reinforcing social norms by trying to relocate that function away from the invisible hand straight into the iron fist of [the State](#).

If the “right” to be forgotten were implemented in any serious way on this continent, then what would the ramifications look like? Would I, as a blogger, be forced by individuals like [Mark Dice](#) or [George Hemminger](#) to remove anything I’ve ever written about either of them, simply because they managed to convince a black robed man to determine that I have violated their “right” to be forgotten? What if other third parties wanted my articles that mentioned [Ron Paul](#) to be cast into the memory hole? Jimmy Wales, co-founder of Wikipedia, [was quoted in The Telegraph](#) as commenting on the “right” to be forgotten by saying:

*“History is a human right and **one of the worst things that a person can do is attempt to use force to silence another.** I’ve been in the public eye for quite some time; some people say good things and some people say bad things. That’s history and **I would never ever use any kind of legal process like this to try to suppress the truth. I think that’s deeply immoral.**”* [emphasis added]

[Historical revisionism](#) is one thing, but outright censorship of the [historical record itself](#) is beyond the pail. Ultimately, that is the slippery slope that the so-called right to be forgotten leads to – “[an amoral, empty, vacuous, soulless, post-modern hell of nothing and no one but the power and the lie of the moment.](#)”

Echoing ex-FTC commish Julie Brills, [John Simpson issued a letter to Google](#) five months after the *González* case, where he said, in part:

“Here is what the Right to be Forgotten is about in practical terms: Before the Internet if I did something foolish when I was young and foolish – and I probably did – there might well be a public

record of what happened. Over time, as I aged, people tended to forget whatever embarrassing things I did in my youth. I would be judged mostly based on my current circumstances, not on information no longer relevant. If someone was highly motivated, they could go back into paper files and folders and dig up my past. Usually this required effort and motivation. As a reporter, for instance, this sort of deep digging was routine for me with, say, candidates for public office. This reality that our youthful indiscretions and embarrassments and other matters no longer relevant slipped from the general public's consciousness is 'Privacy by Obscurity.' The Digital Age has ended that. Everything – all my **digital footprints** – is instantly available with a few clicks on the computer or taps on a mobile device. Now, the Right to be Forgotten is simply restoring the balance in Europe that is provided with Privacy by Obscurity.”

Ah, the ubiquitous [digital footprint](#)! In what is essentially the digital version of a paper-trail, [data traces](#) are those bits of information about you that are created, stored, and potentially analyzed for later use, whether that use be for targeted marketing campaigns or [government manhunts with you as the fugitive](#). Although there are [security culture techniques](#) for mitigating your [digital shadow](#), the fact of the matter is that this “right” to be forgotten is not [a solution to the problem of Big Brother](#), by a long shot.

I think the very worst of the “right” to be forgotten is the development of the *Oblivion* computer program. [About a year ago](#), Simeonovski et. al. birthed this monstrosity:

“We propose a universal framework, called *Oblivion*, providing the foundation to support the enforcement of the right to be forgotten in a scalable and automated manner. Technically, *Oblivion* provides means for a user to prove her eligibility to request the removal of a link from search results based on trusted third party-issued digital credentials, such as her passport or electronic ID card. *Oblivion* then leverages the trust imposed by these credentials to generate eligible removal requests...[i]n *Oblivion*, we use state-of-the-art natural language processing (NLP) and image recognition techniques, in order to cover textual and visually identifiable information about a user, respectively.”

In other words, *Oblivion* streamlines automated takedown requests, for purposes of efficiency, of course. Nothing whatsoever to do with implementing the [Hegelian Dialectic](#) in order to better facilitate the “inconvenient disappearance” of “undesirable” people who find themselves “[black-bagged](#)” by an intelligence agency. Naturally, the designers of *Oblivion* mention how takedowns have to be requested by individuals who would then be required to provide government-issued identification documents, but are they that naïve to simply dismiss how their technology will inevitably be used to conduct [black operations](#)? Thankfully, all that *Oblivion* is proposed to do for now is simply data-mine the information and then red-flag it for analysis by a human being, but seriously, how much tweaking in the program’s source code would need to be done in order to execute an automated takedown **without** an individual’s personal request?

Regarding technological innovations and subversions both, it reminds me of something that the fictional [Foamy the Squirrel](#) character said in a cartoon years ago:

"All you humans are like monkeys with machetes. You people can't even properly utilize the technology you've created."

When those sycophants of authoritarianism beg Leviathan to provide them with legal privileges like the "right" to be forgotten because they were irresponsible enough to not just take a photo of themselves doing something embarrassing, but also upload such a photo onto Fascistbook, it really does reinforce Foamy's observation that the improper use of technology can lead to undesirable consequences. Perhaps humanity is forever doomed to painful transitional stages whenever [creative destruction](#) occurs, yet exacerbating that pain with capricious edicts from the State only deepens the situation that much worse than it really had to be in the first place.

One such edict came from CNIL, which is a French "data protection authority," demanding last year that Google must scrub and delist requested search indices on not just the European extensions of its search engine, as ordered in the 2014 *González* ruling, but worldwide as well. This only further confirms Peter Fleischer's concern that [privacy would be used to justify censorship](#), and that is exactly what the CNIL is actively doing; I bet the next **totalitarian tiptoe** will be when someone uses ["intellectual property" and copyright law](#) to censor whomever is politically vulnerable in the future. All of this is based on the "right" to be forgotten, which if anyone was really being honest, is really nothing more than a government-bestowed privilege.

Some might think that the "right" to be forgotten could be used to lower [recidivism](#), especially in light of [registered sexual offenders and convicted felons](#). Unfortunately, this approach fails to deal with the legal doctrine of [mala prohibita](#), which is why there are more people than ever before whose legal status has been permanently handicapped. If the definitions for what constitutes both felonies (generally) and sex crimes (specifically) is [incrementally expanded over time](#), then don't be surprised when you have more sex offenders and convicted felons as a result of [victimless crimes](#).

Wouldn't it be accurate to say that the only people in today's modern ["society"](#) who truly enjoy the "right" to be forgotten are the [American political prisoners](#)? Once they go in, virtually no one continues to give a crap about them, even if they were "YouTube heroes" before going on the inside. Does that necessarily mean, though, that they are freer than they were before, or even that they enjoy better security culture? I doubt it.

Overall, I think the "right" to be forgotten is less about individual privacy and more about expanding the power of the State. It shows that the EU's judiciary is incompetent, and should not, therefore, enjoy a monopoly on adjudication. Regardless of the aforementioned legal and technical issues, I really believe that the answer to "civil" rights and "positive" liberty is **natural** rights and **negative** liberty (the mashing of the latter pair of concepts would be [natural liberty](#) itself). There is nothing libertarian at all about violating self-ownership under the paper-thin pretext of mitigating the possibility of future prejudice. Rhetoric like that are what self-important celebrities spew, and [Mick Farren and John Gibb had something to say about that](#):

"As celebrities become increasingly paranoid that their cell phones are tapped and their Gulfstreams bugged, it becomes hard for the public to raise a great deal of sympathy for Paris and Michael and Liz and all the other rich-and-famous gossip victims. The prurient public may live vicariously off their antics, but Paris and her crowd are guaranteed incomes far beyond the dreams of avarice to perform those antics. Liz Hurley may have to stand on a bridge to have a private conversation, and Paris Hilton's faux-lesbian photos may hit the Internet, but we more humble mortals are, at the same time, becoming part of databases that will follow us for the rest of our lives – not only without any kind of reward, but often to our total detriment."

Sifting the Wheat from the Chaff: The Value of Skepticism

www.thelastbastille.com/2016/03/02/sifting-wheat-chaff-value-skepticism/

*"How often have I said to you that when you have eliminated the impossible, whatever remains, **however improbable**, must be the truth?"*

– [Sherlock Holmes](#)



Introduction

Sensationalism is the bane of the alternative media. Occasionally referred to as the [Carousel of Carnivores](#), this scourge of misinformation and disinformation is promulgated by “[celebritarians](#)” through the repeater effect. It is because of this that mean world syndrome is promulgated through the [news cycle](#).

Myth-busting has arisen as a reaction to sensationalism. Attempts to use the scientific method to either verify or debunk asserted claims may not be carried out perfectly all the time, yet, the whole exercise shows the value of rationality and empiricism. The success of web series such as [Game Theory](#) (as well as its spinoff, [Film Theory](#)) truly demonstrates the value that both debunking and verification can have for the audience, especially if it's presented in a flashy and attractive style.

As I've mentioned before, [skepticism is healthy](#); unfortunately, in my experience, most “activists” engage in magical thinking, and then they get upset when either they or someone else they know quickly becomes a political prisoner. Skepticism explains *why* wishful thinking is irrational, not to mention the fact that **mythology is the enemy of reason**. Therefore, if you want to lower the probability of individuals going to jail, then you ought to become less gullible.

Good science is *repeatable* and *falsifiable*. It's been said that [the 19th century was renowned for its great skepticism of state power and institutionalized religion alike](#); today's “activism,” by contrast, is mostly unscientific, and what portions of it that are usually tend to be routinely ignored or denigrated simply because they are not overly dramatic or sensationalistic. [Open-source intelligence](#) analysis relies on the scientific method, for without that, whatever

information is gathered by the alternative media becomes automatically discredited by rumors, conjecture, and gossip. Therefore, misinformation and disinformation as promulgated by too many “activists” hurts the practice of good security culture.

Sophistry is, by far, the most dangerous tool used by both reformists and their conspiracist allies in order to mask the truth. Typically, they claim that those who are more deontological (philosophically consistent) are merely “theorists,” and thus not concerned with the real world, yet, when their projects are openly revealed to be notorious failures that are then criticized, they accuse “us” of being cowards (or worse, government agents) for simply not being as foolhardy as they were in their enthusiasm to beg Leviathan for undue favors. I find it rather telling that those who claim their actions are very *practical* are exactly the same ones whose actions are later discovered to be very *impractical*, because they were unsound right from the beginning. They are either fools or liars, but either way, I want nothing to do with them, and in the interest of discovering the truth, I find that I must repeatedly oppose these charlatans. Briefly put, **sophistry is the enemy of the truth**.

Please keep in mind that I will use three **epistemological razors** as the “rules of engagement,” which I will observe in my attempt to guide myself to the truth. **Hitchens’ razor** says that the burden of proof lies solely with the claim maker; it is not incumbent upon skeptics to provide evidence disproving any claims. **Hanlon’s razor** says never attribute to malice that which can be adequately explained by stupidity. **Occam’s razor** says that the simplest explanation is usually the most accurate (put another way, convoluted explanations obscure the truth).

In addition, I will also be using other methods in order to evaluate the truthfulness of various assertions. Cogent reasoning is only possible if I assiduously refrain from committing **illogical fallacies**, even if only inadvertently. Normalcy bias is arguably parallel to confirmation bias, yet both are fallacious and irrational; I can only endeavor to be on the lookout for these and go by what the facts say as best as I can. As implied by the opening quote, the **process of elimination** is an indispensable tool for “**sifting the wheat from the chaff**,” as it were.

If anyone wants to provide rebuttals to my following critiques, then I welcome it. Whether it be due to fallacious analysis or unsound evidence on my part, I sincerely wish rebutters would bring them forward publicly for the edification of the rest of the class, so to speak; **but**, if the evidence is sound, and my reasoning is cogent, *then what I say stands*, which means that if I argue that specific claims are lies, then, most likely, that is the truth of the matter. I am always happy to accept criticism in good faith, but what I absolutely will not tolerate is sophistry from those with ulterior motives, especially if those vested special interests are carried on the winds of political expediency.

One other matter I wish to address before diving headfirst into the swath of claims – I will be assuming that you genuinely care about logic, rationality, and empiricism. If you only value emotive rhetoric and cheap talking points as your guides to what you think of as the truth, then please save yourselves some time by stopping, right now. **I really mean it**: should you be one of those people who puts way too much credence into “muh feels,” you can just piss off, quite frankly. Life is too short to waste precious time and effort on ingrates who shamelessly plop their feces everywhere like savage beasts.

A Brief Review of Patriot Mythology

Last year, Gary Hunt and I did a five-part podcast series entitled, **Patriot Mythology**. Totalling almost six and a half hours, this series exposed and debunked some of the most pernicious lies circulating amongst the American patriot community. Referenced literature was listed and hyperlinked so that the listeners could follow along and verify exactly not only our source documents, but also judge whether our analysis fit the evidence he and I were using to determine the truth.

Simply defined, **patriot mythology** is the collection of unprovable or debunked assertions by constitutionalists about the nature of our political relationship with the several American governments. Although a few of them originally began as simple misunderstandings that were eventually corrected, the majority of these tall tales appealed to the

sensationalistic appetites of those who'd rather financially profit from spreading this folklore rather than restoring limited government, or simply perpetuate the error through lack of understanding. The magnitude of the time wasted by fruitlessly "[debating](#)" on such topics was time and effort *not* spent on more productive tasks.

Three examples ought to suffice for now. Paul Joseph Watson's 2010 article, [U.S. Postal Service Expands Construction of Secret Rooms](#), cried wolf by asserting that some leaked documents proved the existence of (wait for it)...**secret post office torture rooms!** Needless to say, this was complete bollocks, but then again, so is the corporate UNITED STATES myth, which is the bedrock foundation for the oxymoronic "[sovereign citizen](#)" ideology. As if that wasn't bad enough, there are those who still falsely believe that Americans never won the Revolutionary War for Independence, because America is still a British Colony. I know, I know...claims that the British monarchy is controlled by the Vatican is ass-backwards, but this is the nature of patriot mythology – people would rather believe false claims than follow up on the cited sources, even if the bibliography explicitly contradicts the very assertions being made!

Obviously, the importance of [falsifiability](#) cannot be underestimated. If there were to be the three hydras of the digital apocalypse (as illustrated by this article's picture), it would be misinformation, disinformation, and no information. Subsequently, the only way to pushback against these hydras is with the sword of truth, which can only be wielded by those who are being intellectually honest about the subject matter.

So, that concludes my brief review of patriot mythology. Should you desire to learn more, then be sure to listen to the whole podcast series, yet, what I would prefer to do now is to address other myths, which have not been addressed as much as I would have liked, yet are deeply embedded in both patriot and even libertarian circles. My intent by doing so is to, hopefully, enlighten you so that use your own discernment in order to avoid the traps laid by these charlatans.

Brothers-in-Arms?

Groupies are rather annoying, for they insist that membership in their little clicks is all that matters, when in fact the opposite is true. Two of these within the patriot movement are known as the Oathkeepers and the Three Percenters. Oddly enough, they mutually reinforce each other, much like a duality such as yin and yang or male and female.

[Oathkeepers](#) is a nationwide organization composed of active-duty military and law enforcement, as well as first responders (such as fire fighters and paramedics) and veterans, who swore an oath to support the United States Constitution; the organization was founded by Stewart Rhodes in March of 2009. They are most famously known for their [Declaration of Orders We Will Not Obey](#), which outlines the basic tenants of the organization, namely, that they **not** do any of those wretched things on the list. Their assertion for this disobedience to unlawful orders is based upon the idea of the line in the sand.

Right off the bat, you should be able to tell that the main purpose of Oathkeepers, specifically, is to **not do anything!** In other words, American patriots ought to herald these keepers of their oath, so we are told, who remain *bravely neutral* while sitting down twiddling their thumbs. If neutrality were a virtue, then I guess most of the American populace would be composed of *de facto* "oathkeepers."

Additionally, [the line in the sand is a myth](#). Gary Hunt pointed out over two years ago in a stand-alone podcast entitled, [False Hopes: Oathkeepers, Constitutional Sheriffs, & Filming Cops](#), that the Oathkeepers do not care about the practical application of both the Search & Seizure Clause, as well as the Warrant Clause, within the Fourth Amendment to the U.S. Constitution, so he found himself unceremoniously ostracized for testing their integrity. Given that the Oathkeepers do not care about the constitutional limitations found within the Fourth Amendment, do you really think any lines in the sand truly matter to them?

Then there is the issue of the oaths themselves, for which ones are we taking about here? On their "[About](#)"

webpage, the Oathkeepers invoke the Oaths Clause ([Art. VI cl. 3](#)) as the justification behind their whole organization:

“The Senators and Representatives before mentioned, and the Members of the several State Legislatures, and all executive and judicial Officers, both of the United States and of the several States, shall be bound by Oath or Affirmation, to support this Constitution...”

That’s rather interesting, isn’t it? For my purposes in making sense of Oathkeepers, this clause says that all *executive* Officers of the United States (that is, the federal government) and of the several States shall be bound by Oath to support this Constitution. I guess the question at law here is, **who is an executive officer**? I mean, surely Mr. Rhodes isn’t implying that active-duty military and law enforcement, first responders, and veterans are all executive officers of either the United States or of the several States, is he? For that matter, doesn’t Rhodes encourage that the entire federal Congress, plus the legislatures of the several states, as well as all of these judges, to disobey unlawful orders, does he?

Let’s give Rhodes and the Oathkeepers the benefit of the doubt, for perhaps there is another oath they meant to convey. Since two portions of their membership are active-duty military and veterans, it might be a good idea to peruse the [United States Armed Forces oath of enlistment](#), don’t you think? According to [Title 10 United States Code § 502\(a\)](#), it says:

“Each person enlisting in an armed force shall take the following oath: ‘I, _____, do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; and that I will obey the orders of the President of the United States and the orders of the officers appointed over me, according to regulations and the Uniform Code of Military Justice. So help me God.’”

Ah-ha! I knew something was amiss. This enlistment oath establishes a **chain of obedience**, whether it be from the appointed officers or the President himself (pursuant to the [Commander-in-Chief Clause](#)), yet, this still only applies to the federal military, not the government police or anyone else. Also, I don’t see anything referencing “against all enemies, foreign and domestic,” so that must be in yet another oath, right? Well, there is the [Oath of Allegiance](#), which is found at [Title 8 Code of Federal Regulations § 331.1\(a\)](#), which says:

“Except as otherwise provided in the Act and after receiving notice from the district director that such applicant is eligible for naturalization pursuant to § 335.3 of this chapter, an applicant for naturalization shall, before being admitted to citizenship, take in a public ceremony held within the United States the following oath of allegiance, to a copy of which the applicant shall affix his or her signature: ‘I hereby declare, on oath, that I absolutely and entirely renounce and abjure all allegiance

and fidelity to any foreign prince, potentate, state, or sovereignty, of whom or which I have heretofore been a subject or citizen; that I will support and defend the Constitution and laws of the United States of America against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I will bear arms on behalf of the United States when required by law; that I will perform noncombatant service in the Armed Forces of the United States when required by law; that I will perform work of national importance under civilian direction when required by the law; and that I take this obligation freely, without any mental reservation or purpose of evasion; so help me God.' ”

So, although this one too has the “bear true faith and allegiance” phrase just like the Armed Forces oath of enlistment, only this Oath of Allegiance, from what I can tell, mentions the phrase “against all enemies, foreign and domestic.” Man, I guess those naturalized immigrants must be pretty gung-ho on that all that Americana, maybe even more so than those natively-born enlisted men? In any case, I don’t think the Oathkeepers have met their burden of proof here, nevermind when it comes to law enforcement.

Between three different oaths to the federal government, I can’t tell which one is controlling for the Oathkeepers, whether it be the Oaths Clause, the Armed Forces oath of enlistment, or the Oath of Allegiance for naturalized immigrants. This is rather problematic because it’s even more foundational than their list of orders they’re more than happy to disobey, especially considering that keeping one’s oath is *the very purpose of the organization itself*! Not only should you be asking, “Which oath?,” but also the question, “[Which constitution do they support?](#),” especially considering [the Three Constitutions problem](#).

At the risk of further belaboring the point, since I was a former Boy Scout, does that mean that I, too, am an oath-keeper (that is, a keeper of my oath)? The [Boy Scout Oath](#) says:

“On my honor, I will do my best, To do my duty to God and my country and to obey the Scout Law; To help other people at all times; To keep myself physically strong, mentally awake, and morally straight.”

Given that I’ve been inactive with the BSA for over a decade now, does that mean I have kept my oath? I had to recite that oath at the beginning of every troop meeting, as well as at other times and events, all throughout my teenage years, while wearing the uniform. I’d like to think that being a content producer within the alternative media has served as a way for me to continue to remain “mentally awake and morally straight,” at the very least. You, the reader, should make the decision as to whether you think I’ve kept my oath, if oath-keeping is to have any meaning, or credibility, at all.

What have been the activities of Oathkeepers, other than **not** participating in tyranny? It would seem to be the case that one of them was their infamous cowardly retreat during the Cattle Unrustling at the Bundy Ranch due to what was later exposed as a fake drone attack. I remember watching the debrief report where one of Rhodes’ flunkies, Robert Casillas, [chewed out Ryan Payne](#) for leading the militiamen in a vote as to whether the Oathkeepers should be ostracized from the Bundy Ranch, [which they did](#). Is it really any wonder then that [Adam Kokesh cut up his Oathkeepers’ membership card](#) when Stewart Rhodes opposed his proposed armed march into the District of Criminals? Hell, [Oathkeepers specifically condemned Ammon Bundy’s sit-in](#) at the Malheur National Wildlife Refuge earlier this year.

Whether it be Bundy Ranch, the July 4th armed march (that never happened), or the sit-in by the [Citizens for Constitutional Freedom](#), Oathkeepers does appear to have a habit of **not** participating in activities involving gun owners, so I will give them that. It is because of this opposition to patriots, and libertarians alike, that Oathkeepers have been derisively referred to as the “oath-breakers,” which is a moniker I think they’ve earned.

[Three Percenters](#), on the other hand, were supposed to be the more “hard-core” version of Oathkeepers. Mike Vanderboegh, the founder of the Three Percenter concept, [describes it thusly](#):

“During the American Revolution, the active forces in the field against the King’s tyranny never amounted to more than 3% of the colonists. They were in turn actively supported by perhaps 10% of the population. In addition to these revolutionaries were perhaps another 20% who favored their cause but did little or nothing to support it. Another one-third of the population sided with the King (by the end of the war there were actually more Americans fighting FOR the King than there were in the field against him) and the final third took no side, blew with the wind and took what came.”

This is a rather fascinating claim, especially considering that there are no source citations provided by him anywhere on his [Sipsey Street Irregulars](#) blog that I can find. Given that this is falsifiable, I decided to explore the historical validity, if any, behind Vanderboegh’s foundational assertion.

Both a modern historian and a Founding Father appear to be at odds with the historicity of Vanderboegh’s justification for the Three Percent. Robert Calhoun wrote in [his 2008 book on the American Revolution](#) that:

“The loyalists were colonists who by some overt action, such as signing addresses, bearing arms, doing business with the British Army, seeking military protection, or going into exile, supported the Crown during the American Revolution. Historians’ best estimates put the proportion of adult white male loyalists somewhere between 15 and 20 percent. Approximately half the colonists of European ancestry tried to avoid involvement in the struggle – some of them deliberate pacifists, others recent emigrants, and many more simple apolitical folk. The patriots received active support from perhaps 40 to 45 percent of the white populace, and at most no more than a bare majority. Amerindians split into the same pro-British, pro-American, and neutralist alignments, with those tribes that British Indian Super-intendents since the 1740s proving most likely to support British arms.”

If accurate, then I’m not sure why Vanderboegh would say that the Three Percent received assistance from the 10% of the populace whereas Calhoun said they received at least 40% from the other colonists; but hey, perhaps Calhoun and Vanderboegh are off base on their estimates? What better educated guess could be provided by anyone other than straight from John Adams? According to [the Little, Brown & Co.’s 1856 publication of his letters](#) (alongside a biography written by his grandson, Charles Adams), John Adams wrote the following to [Thomas McKean on August 31st of 1813](#):

*“Upon the whole, if we allow two thirds of the people to have been with us in the revolution, is not the allowance ample? Are not two thirds of the nation now with the administration? Divided we ever have been, and ever must be. **Two thirds had and will have more difficulty to struggle with the one third, than with all our foreign enemies.**” [emphasis added]*

Adams rightly admonished McKean for naïvely proselytizing that “the great mass of the people” were supportive of independence as early as 1765, because if that were true, then how do you explain the urgency of Thomas Paine’s arguments that he presented in his 1776 [Common Sense](#)? Besides, at best, this would only mean that ~ 33% of the colonists supported independence, not anything in terms of those proportions who served in combat versus logistics or some other supportive function, as Vanderboegh claimed. Furthermore, Adams wrote the following [to James Lloyd in January of 1815](#):

“If I were called on to calculate the divisions among the people of America, as Mr. Burke did those of the people of England, I should say that full one third were averse to the revolution. These, retaining that overweening fondness, in which they had been educated, for the English, could not cordially like the French; indeed, they most heartily detest them. An opposite third conceived a hatred of the English, and gave themselves up to an enthusiastic gratitude to France. The middle third, composed principally of the yeomanry, to the soundest part of the nation, and always averse to war, were rather lukewarm both to England and France; and sometimes stragglers from them, and sometimes the whole body, united with the first or the last third, according to circumstances.”

Of course, it is not the American Revolution that Adams is addressing here, but the *French* Revolution, since Americans were bellyaching over whether or not to support the [Jacobins](#). As Michael Schellhammer [wrote in his article on February 11th of 2013](#):

*“Truth is, Adams was not addressing America’s rebellion – he was writing about American attitudes towards the French Revolution, when Americans grappled with either supporting France or maintaining commercial ties with Britain. The mistake appears to stem from historian Sydney George Fisher, who misinterpreted Adams’ meaning in his 1908 book, *The Struggle for American Independence, Volume I*. Others, reading the quote without the full context of Adams’ letter, **have repeated the error ever since.**” [emphasis added]*

So, whether it stems from a misunderstanding of *whose* revolution we’re talking about, or from the simple inability to *do basic math*, Vanderboegh’s promotion of this Three Percent is outright mythical, just like “[the line in the sand](#)” or the “[corporate UNITED STATES](#).” History does not support Vanderboegh, which just might explain why he lacked any source citation for the foundational assertion of the Three Percenters in the first place.

Yet, the sheer lack of historicity isn't the only problem to deal with here, for there is the question of whether the Three Percenters are an organization. Vanderboegh himself wrote in both [2010](#) and [2014](#), respectively, that:

"The Three Percent is NOT an organization. That would be too easy to kill, too simple to discredit. The Three Percent is an idea, a movement of like-minded people, and that is something that is far harder to kill. Almost impossible, really."

"The Three Percent idea, the movement, the ideal, was designed to be a simple, powerful concept that could not be infiltrated or subjected to agents provocateurs like many organizations that I observed in the constitutional militia movement of the 90s."

This would seem to imply that the Three Percenters, as an abstract idea, is more along the lines of [leaderless resistance](#), but such is not the case in practice. To start with, there are websites and groups such as [Threepercenter.org](#), [Three Percenter Nation](#), [Three Percenters Club](#), [Oregon Three Percenters](#), and the [Idaho Three Percenters](#). Secondly, does it make sense for any Three Percenters to have "use permits" for [protesting](#)? As [Brandon Curtiss announced from the bed of a pickup truck](#):

"The parade route...there will be people, like I said, placed at the stop lights, we have to observe all the traffic laws, that was the one request we had from the Boise police department. We do have a use permit for doing what we do, so we're all good to go. We just can't obstruct traffic."

I remember [Naomi Wolf](#), of all people, being against the whole idea of a "protest permit," yet Brandon Curtiss seemed to have taken it as a matter of course. Last November, the Idaho Three Percenters held their "Idaho First!" rally in order to protest the [Syrian refugee crisis](#), which is indicative to me of [the neocon infiltration of the patriot movement](#). If accurate, then this would contradict Vanderboegh's claim that the Three Percenters were immune from infiltration.

Speaking of the Idaho Three Percenters, I think it would be relevant to mention the provocateuring in Harney County, Oregon as of late. First, a ["buffer zone" was originally promised by Brandon Curtiss](#), at least, until he and his crew left Oregon to go back to Idaho; this left one of the Final Four at the Malheur National Wildlife Refuge, [Sean Anderson](#), asking the question of [where is the buffer zone that was promised?](#) Secondly, it was none other than Brandon Curtiss who launched ["Operation Freedom Ride,"](#) which quickly became the now infamous dildo fundraiser, whose proceeds went directly to the Idaho Three Percenters (this is why the Three Percenters are now referred to derisively as the "Three Inchers"). Thirdly, it was [Brandon Curtiss and his thugs who harassed and tried to intimidate Gary Hunt](#) while he was in Burns, but this provocateur was thankfully scared off by at least two other American patriots in the vicinity.

A match was made in hell during the aftermath of last year's [Chattanooga shootings](#). Stewart Rhodes issued an Oathkeepers "national call to action," which launched [Operation Protect the Protectors](#). This was an effort to guard the military recruitment stations from any further Islamic terrorism – an effort that was specifically rebuked by the U.S. Army, where they went so far as to say that [recruiters must treat armed citizens as a security threat](#).

Interestingly, some Three Percenters joined in this “operation” to guard the military recruitment stations.

So, it would seem to be the case that when the militiamen protecting the Bundy Ranch could use whatever help was available, the Oathkeepers fled. When the Final Four were holding out at the refuge, the Three Percenters fled. Yet, when a lone Islamist attacked the federal military, both the Oathkeepers and Three Percenters couldn't stumble over themselves quickly enough in order to volunteer for guard duty. Why bother [protecting private property for profit](#) when it's so much more acceptable to guard government property for free?

After observing their behavior and the foundational claims behind their respective organizations, I'd have to conclude that, yes, the Oathbreakers and the Three Inchers are certainly “brothers-in-arms” with each other, but certainly not with the American patriot movement, because whenever given a chance, not only would they rather commit desertion, but also actively lend support to the federal government, even when it's repudiated by Leviathan itself.

Now, I ask you, how is this any different from what [Mark Kessler](#) did?

“Anti-Government” Government Agents?

Speaking of Mark Kessler, there is a rather dangerous presumption made by most constitutionalists that for some inane reason, American patriots ought to collaborate with the government employees of the several state governments. The idea here is to use the several states of this highly overrated Union as a bulwark against the central government headquartered in the District of Criminals. Two distinct, yet overlapping, approaches to doing just this are what are known as “constitutional” sheriffs and state “nullification.”

Constitutional sheriffs are thought of as those county sheriffs who honor their oaths of office (sound familiar?). [Three years ago](#), this “constitutional sheriff-ing” was expressed by county sheriffs who professed to uphold the right to keep and bear arms by refusing to enforce unconstitutional gun control, particularly in the form of executive orders. As can be expected, nothing came of this, although there have been some recent concerns following [the President's infamously weepy press conference](#) that perhaps he might try to make one final effort to push through some gun control during his last year in office.

What legal basis, if any, does this notion of “constitutional” sheriffs have in the government's own laws, though? There is nothing enumerated in the federal Constitution about sheriffs, so the Tenth Amendment refers you to your most relevant state constitution. For me, this would be the [1876 Texas Constitution](#), which enumerates sheriffs only a few times I could find that I will list here for your delectation:

- Art. III § 52e: “Each county in the State of Texas is hereby authorized to pay all medical expenses, all doctor bills and all hospital bills for Sheriffs, Deputy Sheriffs, Constables, Deputy Constables and other county and precinct law enforcement officials who are injured in the course of their official duties...”
- Art. V § 23: “There shall be elected by the qualified voters of each county a Sheriff, who shall hold his office for the term of four years, whose duties, qualifications, perquisites, and fees of office, shall be prescribed by the Legislature, and vacancies in whose office shall be filled by the Commissioners Court until the next general election.”
- Art. VIII § 14(b): “In any county having a population of less than 10,000 inhabitants, as determined by the most recent [decennial census of the United States](#), the sheriff of the county, in addition to that officer's other duties, shall be the assessor-collector of taxes, except that the [commissioners court](#) of such a county may submit to the qualified voters of the county at an election the question of electing an assessor-collector of taxes as a county officer separate from the office of sheriff. If a majority of the voters voting in such an election approve of electing an assessor-collector of taxes for the county, then such official shall be elected at the next general election for the constitutional term of office as is provided for other tax assessor-collectors in this state.”

- Art. XVI § 1(a): “All elected and appointed officers, before they enter upon the duties of their offices, shall take the following Oath or Affirmation: ‘I, _____, do solemnly swear (or affirm), that I will faithfully execute the duties of the office of _____ of the State of Texas, and will to the best of my ability preserve, protect, and defend the Constitution and laws of the United States and of this State, so help me God.’ ”
- Art. XVI § 1(b): “All elected or appointed officers, before taking the Oath or Affirmation of office prescribed by this section and entering upon the duties of office, shall subscribe to the following statement: ‘I, _____, do solemnly swear (or affirm) that I have not directly or indirectly paid, offered, promised to pay, contributed, or promised to contribute any money or thing of value, or promised any public office or employment for the giving or withholding of a vote at the election at which I was elected or as a reward to secure my appointment or confirmation, whichever the case may be, so help me God.’ ”

What this seems to mean is that Texas county sheriffs are constitutionally enumerated to be elected for four-year terms by the electorate, to collect taxes in lower populated counties, to enjoy taxpayer-funded medical care, and to have sworn an oath to uphold federal laws. So, that is what a “constitutional” Texas county sheriff is – **a politician with a tin badge on his chest.**

Constitutionality aside, perhaps these county sheriffs can still serve as a bulwark against the federal government because their financial incentives lie with the Texas government? *Au contraire*, naïve patriot, for the phenomenon of “[greenmail](#)” ensures compliance with federal demands, as does the “[equitable sharing](#)” provisions integral to [civil asset forfeiture](#). I can’t imagine county sheriffs respecting your natural liberty as they engage in “[policing for profit](#)” while simultaneously receiving kickbacks from the federal government.

But wait, isn’t it possible for corrupt sheriffs to be unseated if a good citizen ran for sheriff and won the election? Ah, well, Anthony Bosworth tried doing that in Yakima County, Washington last year – although [Bosworth admitted he lost the election](#), he oddly bragged that he “broke records.” Naturally, Texan candidates for sheriff must be registered voters, so in light of the fact that I’m an “[ex-voter](#),” I am ineligible to run for [the office of any Texas county sheriff](#).

More significant than ulterior financial motives or the viability of [running for public office](#), though, is the constitutional [monopoly on policing](#) itself. Thankfully, [most cops are not constitutional](#) (municipal police, state highway patrol, and the federal alphabet soup boys are not enumerated in any American constitution I’ve ever read), but just because something is constitutional does not therefore mean it is ethical. [Monopolies have been authorized by the federal Constitution](#), so the promoters of “constitutional” sheriffs, such as the [Constitutional Sheriffs and Peace Officers Association](#) (CSPOA), totally dodge any moral or economic criticisms about [the monopoly on the production of security services](#), simply because the state constitutions said so, and that’s all you need to know, according to them. Obviously, such avoidance by the CSPOA of these serious critiques to their constitutionally enumerated monopoly indicates their failure to bear the burden of proof.

Similar in spirit to the “constitutional” sheriffs is the purported method of state “nullification.” [Dr. Tom Woods](#) is the foremost academic on the subject; in brief, Dr. Woods spends the majority of ink on the page attempting to bear his historical burden of proof, which although I appreciate the effort, there was virtually no helpful information on how to practically make this technique work in the present. The best he can do is to tell you to write your legislator and to desperately plead for the legislature to “nullify” *unfunded* federal mandates, to repeal the 17th Amendment (somehow), and to establish federal tax escrow accounts – this last item, ironically, violates the Appropriations Clause ([Art. I § 9 cl. 7](#)).

Ignorance of [the ratification period](#) by most constitutionalists might just explain why some of them advocate for state “nullification.” The Tenth Amendment was only possible because of the Anti-Federalists, which is particularly important when you consider that Alexander Hamilton staunchly opposed any bill of rights in [Federalist Paper #84](#), on the unbelievably lame excuse that Articles I – VII **were already** a bill of rights. Worse, there were [three and a half years between the ratification of the Constitution and the Bill of Rights](#); interestingly enough, the Whiskey Rebellion took place during this interim when the hated whiskey tax was passed into law during March of 1791. In light of these

facts, why these “Tenthers” revere the Constitution is beyond me.

State “nullification” inherently relies on a combination of [grassroots lobbying](#) and running for public office, besides [electoral voting](#). These methods are used to encourage a state legislator to introduce a bill into the legislature of which he is a member, and once that bill is signed into law by the governor, then this new statute is said to “nullify” the federal one, since they contradict each other; because of this, state “nullification” is inherently reformist, much like [jury nullification](#). No wonder [cancelling your voter registration](#) is such a threat to the false perception that [reformism](#) is effective and practical in restoring liberty.

Before perusing the efficacy of modern state “nullification” in Texas, I would like the Tenthers to answer two questions regarding this technique. They are:

1. Who has the power to use state nullification against the federal government?
2. What *exactly* is the motive for this actor to nullify unconstitutional federal actions?

When you consider that Art. XVI § 1(a) of the Texas Constitution applies to legislators as elected officers (presumably just the same as county sheriffs), then why should you expect these legislators to nullify federal laws that they have sworn in their oaths of office to uphold? I find it quite revealing that [Dr. Woods prefers to swat against baseless accusations](#) of racism, or of being a “neo-Confederate,” yet neglects to address these pivotal questions I’ve raised.

Empirically, there are three questions that should be answered in order to determine the usefulness of state “nullification.” Briefly, they are:

1. How successful has Michael Boldin’s Tenth Amendment Center (TAC) been in encouraging the use of state nullification?
2. How many federal laws have been successfully nullified by the several state legislatures?
3. How much time do Tom Woods and Michael Boldin need in order to fully test the viability of modern state nullification?

I’ll attempt to answer these questions in reverse order. First up, you must consider that the TAC was founded back in 2007; this means that Boldin has had 9 years to test the current viability of state nullification. To be fair, [FIJA has had 27 years](#) to test the efficacy of modern jury nullification, yet, I think nearly a decade of advocacy is plenty of time by which to gauge a method’s efficacy. Now, in order to address the sheer amount of federal laws nullified, I will limit myself to Texas, just for the sake of simplicity. According to the [“Tenther Action Center,”](#) the [2015 State of the Nullification Movement report](#), and the [TLO database](#) (which is the Texas legislature’s bill tracking system), I’m able to determine what legislative bills got passed into law. In summation, they are:

- “Right to try” experimental medications ([HB 21](#))
- [Texas Bullion Depository](#) ([HB 483](#))
- [Licensed open carry of “handguns”](#) ([HB 910](#))
- Common Core prohibition ([HB 642](#))
- Drone surveillance prohibition ([HB 912](#))
- Automatic license plate reader regulations ([SB 1286](#) & [HB 2876](#))

Of these, only the license plate ones died in committee, so all the rest were signed by the governor; however, was their success really attributable to state nullification? Although HB 21 is a pushback against *some* FDA “regulations,” they are only applicable to *terminal* patients. HB 642 and HB 912 are prohibitions against the use of the Common Whore “standards” in Texas [public schools](#) and the use of drone surveillance by the Texas police, respectively; I’m not quite sure what the federal government’s intervention is here, exactly. HB 483 just establishes another

government entity, so I'm not sure why the Texas Bullion Depository is a pushback against central banking. Finally, HB 910 is a pushback against Art. I § 23 of the Texas Constitution, [not the Second Amendment](#), so that one definitely doesn't count as state "nullification," unless Tenthers would have you believe that the legislature can "nullify" its own constitution.

This suggests to me that the TAC, while admirable in their attempt to try something creative, was at best, an experiment, or at worst, a false hope; either way, I think the results are pretty clear. Granted, I would encourage anyone who wants to replicate what I've outlined here to do so with where they live, and see whether or not they get similar results. If TAC is said to be "successful" regarding state "nullification," it would be in an **educational** context, but not in a practical sense by any means. In my not-so-humble opinion, state "nullification" is nothing other than a version of a theme of jury nullification trying to rear its ugly head once again in order to [rope political dissidents back into counter-productive reformism](#).

What can be learned from the folly of both "constitutional" sheriffs and state "nullification" is that you should not place so much faith in the efficacy of the Tenth Amendment, or "your" respective state constitution, for securing your liberties. From what I can tell, Art. XVI § 1(a) subjugates Texan government employees to the jurisdiction of the federal government; if accurate, then you cannot trust either county sheriffs or state legislators to restore your liberty for you. Needless to say, these two ideas are just more expressions of reformism, and it's really quite pathetic that constitutionalists and libertarians alike believed this tripe – maybe both of them were more gullible than I had initially presumed.

Anarchist Mythology

Speaking of libertarians, they are not immune to their own mythologies, as some would have you falsely infer that only the American patriots were superstitious. Wishful thinking is a plague upon an individual's consciousness, for it mutates their sincere desires into fallacious nonsense. Two pernicious concepts that are quite popular amongst libertarians and anarchists are the Philadelphia Conspiracy and "peaceful" parenting.

Revisionist history is not a plight upon the truth *if* the facts are accurate. Simply put, this idea of the Philadelphia Conspiracy is traceable back to L. Neil Smith's 1980 novel, [The Probability Broach](#), which describes the "conspiracy" thusly:

"The fiend responsible for this counter-revolutionary nastiness was Alexander Hamilton, a name Confederates hold in about the same esteem as the word 'spittoon.' He and his Federalists had shoved down the country's throat their 'Constitution,' a charter for a centralist superstate replacing the thirteen minigovernments that had been operating under the inefficient but tolerable Articles of Confederation. Adopted during an illegal and unrepresentative meeting in Philadelphia, originally authorized only to revise the Articles, this new document amounted to a bloodless coup d'état."

Keeping in mind that this is [historical fiction](#), the ratification period is depicted in a rather sinister light. Had this black portrayal of the 1780s been left treated as harmless entertainment, then that would have been the end of it, but the problem here is that there were libertarians who thought they saw some truth in what Smith's characters were saying. Obviously, [I am no longer a fan of the United States Constitution](#), yet, I am compelled by my appreciation for intellectual honesty to debunk this alleged conspiracy, hopefully once and for all.

The basic assertion of the Philadelphia Conspiracy is that the Framers of the U.S. Constitution executed a [coup d'état](#) against the American colonists through deceit and guile. What's far scarier, I suspect, is the sheer horror of the fact that the Anti-Federalists *compromised* with the Federalists by persuading them to have the Bill of Rights ratified following the ratification of the Constitution; in other words, the Anti-Federalists sold out, hence why the Constitution is sometimes referred to as the Great Compromise. I can prove this with the very existence of the [The Anti-Federalist Papers](#) – it is a bit dishonest to claim, on the one hand, there was a “bloodless coup d'état,” yet on the other hand, there exists a record of public discourse about whether or not to ratify the Constitution that spans two years.

Conspiracists cannot have their cake and eat it, too. They cannot use a *fictional novel* against *historical documents*, and then claim that the assertions in the novel trump the documentation. To paraphrase a line from [V for Vendetta](#), artists use lies to tell the truth, whereas politicians use lies to cover the truth up. Again, [I've written some libertarian fiction myself](#), but I have no interest in covering up the truth (the mainstream media does that well enough without my help), so the promoters of the Philadelphia Conspiracy act more like oxymoronic “[anarchist politicians](#)” rather than libertarian artists.

Paralleling these conspiracists within libertarian circles are [the advocates of “peaceful” parenting](#). I've read their recommended literature, which includes Lloyd de Mause's [The Origins of War in Child Abuse](#), Dr. Murray Straus' [Beating the Devil Out of Them](#), and Drs. Neufeld and Maté's [Hold Onto Your Kids](#), and I must admit, I remain thoroughly *unconvinced* that [spanking is a form of child abuse](#). I have no reason to think that spanking violates the non-aggression principle, and I will remind my readership that the burden of proof lies squarely upon the shoulders of the “peaceful” parenting advocates to demonstrate that to be the case.

To me, it would seem that the “peaceful” parents violate Hanlon's razor by ascribing a malicious intent upon nearly all parents when much of their behavior and motives could be described as stupid (much like Leviathan, in some respects). For instance, deMause spends the majority of his book detailing grotesque acts of pedophilic rape and sexual torture, but then mentions that the evolution of childrearing psychogenic modalities has *improved* while overall human violence has dramatically *declined* over time. Spanking was only mentioned twice in passing, and deMause did *not* recommend *any* non-spanking forms of child-rearing *at all*, much like [the Lysander Spooner routine](#) of expressing a grievance without so much as offering an alternative solution, or option, to alleviate the suffering in question. This really makes me wonder as to why the “peaceful” parenting advocates recommended deMause's book to further their cause, since he had virtually nothing to say about spanking in the first place. Ulterior motives, much?

Meanwhile, there appears to be an implied unholy alliance between the “peaceful” parenting advocates and [Child “Protective” Services](#). Dr. Straus was very much in favor of the [infamous Swedish 1979 anti-spanking law](#), despite the fact that one of the unintended consequences was the police round-up of Aziz Raheem Awalludin and his wife, Shalwati Nurshal, who were arrested by the Swedish police over two years ago for slapping their then-12-year-old son's hands, under auspices of the anti-spanking law. I must ask, why aren't the “peaceful” parents not more outspoken against CPS? To my knowledge, only [Kal Molinet](#) and [Justus Ranvier](#) are the sole [voluntaryists](#) who've advocated on behalf of “peaceful” parenting *and* specifically repudiated the CPS.

[Adam Kokesh's comparison of parenthood to government tyranny](#) is hugely misplaced. To reiterate my criticism to his arguments, when people beget children, they hung around their own neck the obligation of raising them, simply because they directly participated in creating their very lives, to put it delicately. Parents are the *guardians*, not the owners, of their children, and as such must respect their individual self-ownership (just as libertarians do); however, until those children become adults, their exercise of free will must necessarily be curtailed since they typically lack the capacity for personal responsibility that comes along with individual liberty.

To illustrate but just one [non sequitur fallacy](#) commonly held by “peaceful” parenting advocates, just because parents chose to beget children does not therefore mean children are equal in status to adults. Yes, they are human, and yes, they enjoy the same natural liberty you and I do. Put another way, children, just like adults, only enjoy

negative liberty, that is, the freedom to *not* be arbitrarily punished, or otherwise interfered with. Thus, any housing, food, education, or any other goods or services bestowed on the child by the parent is simply little else than a debt incurred when the parent in question reproduced, yet even this is primarily limited to the nature of their relationship being a *temporary guardianship*. Once the child has demonstrated the maturity of an adult, regardless of whether his age be 12 or 25 years old, the two individuals in question now enjoy something resembling an “equal” relationship, particularly with regards to its voluntariness, even if they don’t like each other, in which case [ostracism becomes an option](#).

Although the involuntary position of the child with regards to his parents is blatantly obvious, the reciprocal obligations between parent and child (that is, a duty of upbringing and rearing in exchange for a duty of obedience within reason) is, all things considered, not entirely unreasonable or inequitable, especially on behalf of the child, in the absence of coercion by the parent. Obviously, this is not an exhaustive *a priori* reasoning of the parent-child relationship, but I hope it will suffice for now. Unfortunately, what is deceptively being pushed here by the not-so-peaceful parenting advocates is an “egalitarian” agenda to undermine parental rights, even if only unwittingly, yet I attribute that to stupidity on the part of the “peaceful” parenting advocates, not malice, especially considering that more than a few of them, oddly enough, are themselves childless.

Thankfully, there is now some pushback by libertarians against the diatribes of the “peaceful” parenting advocates. [Lenore Skenazy](#), an advocate for [free-range parenting](#), recently [said the following in response to an interview question by Shane Radliff](#) as to whether she thinks that spanking is a form of child abuse:

*“I think everybody knows the difference between a spanking and child abuse, it’s obvious. Abuse is cruelty, it’s just taking something out on a kid, whereas spanking, once in a while, if you have to spank a kid – I haven’t spanked my kids, but I remember being spanked a little bit, and I think that if the child knows that you love them and knows that you care about them – like I said, when we have to swoop in is when children are beaten, when they are starved, when they are given drugs, and when they are pimped out, and I think we all know the difference between true abuse and a difference in parenting styles...we’re all different, and it doesn’t make a difference if you’re showing your kid that you love them and you’re making sure that they get fed – from there on out, **let’s give everybody the benefit of the doubt**, that they are doing the best that they can.” [emphasis added]*

As you can tell, Skenazy takes the *opposite* position of the “peaceful” parents who froth at the mouth that child abuse is rampant. [Tilting at windmills](#) is what the “peaceful” parents seem best skilled at doing, alongside their [“doom porn” aficionado](#) counterparts. Both of them utterly fail at constructing rational models of security because they prefer to let their intuitive *feelings* about security distort the actual reality of security, which is exactly what Bruce Schneier warned against back in 2010.

From my vantage point, any collusion between the Philadelphia conspiracists and the anti-spanking advocates is really only indicative of the irrationality within libertarian circles that pops up occasionally. Neither of them have abided by Hitchens’ razor in bearing their burden of proof, and so I am left to conclude that the only reason either of them are given the time of day is because they feed the confirmation bias some libertarians vainly seek in their attempts to delegitimize the State. I fail to understand why some anarchists would be so willing to collectively demonize parents or spread misinformation about the Framers of the U.S. Constitution as part of their efforts towards abolishing the State, when there are far more reasonable and effective ways to do just that, such as the [strategic withdrawal strategy](#), which was first alluded to by [Étienne de La Boétie in 1576](#).

Conclusion

After covering a swath of myths and half-truths permeating throughout the alternative media, it becomes pivotal to understand the popularity of these rumor mills, and who benefits from spreading such misinformation. The magnitude of the time and effort spent “debating” on such topics is time and effort *not* spent on more productive tasks. Lack of rationality, coupled with ulterior political motives, gives rise to a [society of the spectacle](#) where reality matters not.

Whether it be due to sensationalism or “[conspiratainment](#),” I regret to admit that the independent media is now slowly morphing into an Internet version of the corporate mainstream media. I still think, perhaps naïvely, it is possible for the remnants of the free press to turn that trend around, but to do so would require a serious all out effort to immediately reinvigorate that classically liberal value of **skepticism** before it’s too late and the irrational superstitious nonsense engulfs the whole [blogosphere](#). Occam’s razor is like holy water to the shameless promoters of all this claptrap, whether it be that [Antonin Scalia was murdered](#) or the fake Muslim “invasion.”

Gullibility *lowers* your capacity to exercise your freedom, because it skews your **security assessments** (which is composed of [threat modeling and risk analysis](#)) towards fallacious conclusions that, in turn, leads to terrible security culture, and ultimately, a *higher* likelihood of becoming a [political prisoner](#). Debunking myths is very much a game of “whack-a-mole,” albeit with the challenge being that nobody has enough time in the day to “put out (all the) fires” caused by sensationalists and conspiracists who seek to benefit from the resulting chaos, especially in some form of monetary compensation or just narcissistic self-aggrandizement. My intentions have been to present before you a wide variety of myths that, much like doom porn, only serve to increase your [opportunity costs](#).

Oathbreakers, Three Inchers, “constitutional” sheriffs, state “nullification,” the Philadelphia Conspiracy, and “peaceful” parenting *all* violate, both in difference of kind and of degree, some combination of the three epistemological razors I’ve measured them by – Hitchens,’ Hanlon’s, or Occam’s razors. None of these six myths pass my own “smell test,” and thus, I feel duty bound to maintain my integrity by specifically rebuking each of them, so that there can be intellectual honesty between the different kinds of people within the alternative media, including both content producers and the audience, regarding where the discovery of truth leads us in understanding this reality.

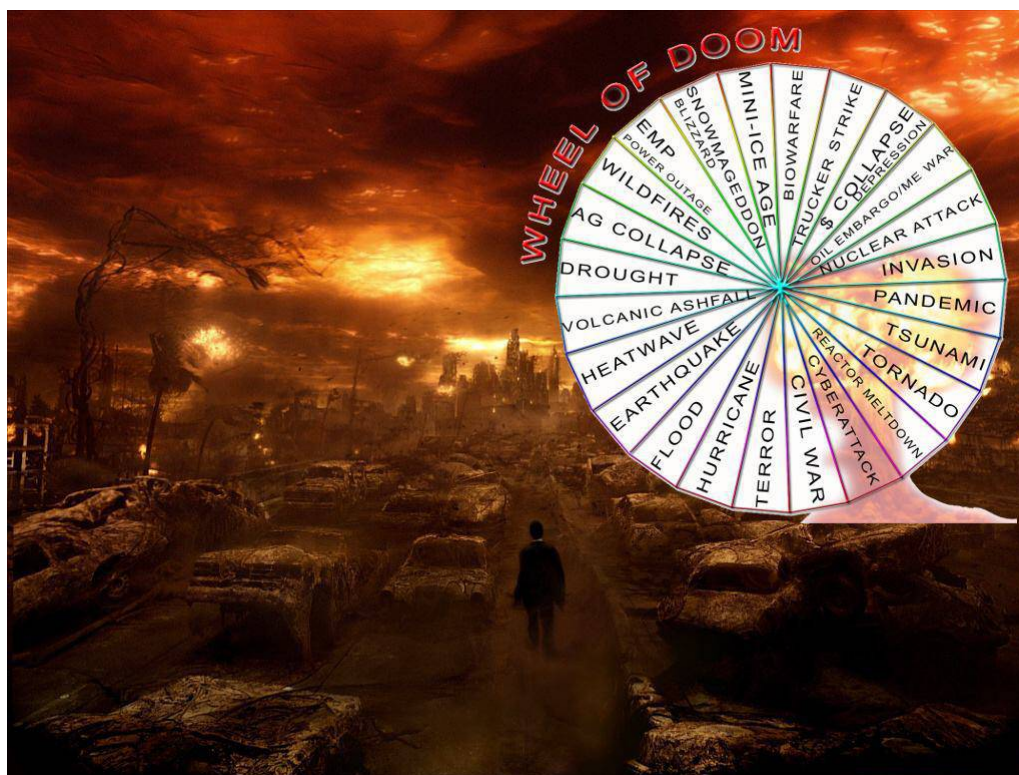
Naturally, I encourage all of you to take what I have offered here and subject it to your own reasoning and empiricism. It is my hope, and prayer, that once you possess this knowledge and new insight, that at least several, if not many, of you will act in your own best interests by not believing these mythologies as if they were true. Finally, [as The Anti-Terrorist so wonderfully explained back in 2010](#):

“Your job is to recognize the real threats amongst the media distractions and irrelevant issues. Ultimately, you’re going to have to rely on your own discernment regarding how important these issues actually are, then make your own decisions and choices accordingly. I doubt many of you will see things exactly as I do, but hopefully you’ll learn from considering my point of view. Even the things that you disagree with will be helpful because it might get you to reassess your own view, then make the right decision for you in your own circumstances. Work hard at making sure that you’re correct in your views and always try to keep an open mind, so that the new or changing evidence isn’t going to be overlooked.”

Modeling Threats & Analyzing Risk: A Rebuttal Against “Doom Porn”

thelastbastille.wordpress.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/

Individual cognitive traits possess a high degree of variety amongst humans. Institutions, such as organized religion and corporate media, take advantage of the predilection some folks have for immersing themselves in speculative fantasy; consider the popularity of television shows like *Jeremiah*, *Jericho*, and even *The Walking Dead* franchise. The problem here, though, is that hypothetical lifeboat scenarios encourage people to reorient their entire lives around waiting (or “preparing”) for their calamity to occur, usually at the expense of everything and everyone else in their lives.



Bruce Schneier gave a lecture at [TEDxPSU](https://www.tedxpsu.org/) back on October 10th of 2010 entitled, “[Reconceptualizing Security](#).” His thesis was that we should bring our intuitive feelings and rational models of security in line with the objective reality of security, because for the most part, the typical feelings and models are not consistent with reality. Humans make security tradeoffs all the time in order to survive, but there is a tendency to exaggerate infrequent, unknown, personified, or uncontrollable risks while downplaying common, known, anonymous, or manageable risks. In other words, risk analysis can be irrationally skewed by not only [confirmation bias](#), but also by [normalcy bias](#).

Rolf Dobelli that same year explained why the [news cycle](#) is detrimental to an individual’s sense of reality. Not only does the news feed confirmation bias, but it also skews risk analysis, mainly because it fails to

explain the underlying processes at work. While I do appreciate the good faith effort in revitalizing the practice of citizen journalism, not everybody in the alternative media provides quality reporting, as evidenced by the [opportunity costs](#), [physiological addictions](#), and [learned helplessness](#) observed in some consumers of [new media](#). Put another way, the news encourages incorrect threat modeling due to its pandering to the [availability heuristic](#).

[Eric English](#), a survivalist vlogger, has taken issue with the way most “preppers” rationalize their activities in terms of coping with their own pet visions of “doomsday.” His thesis appears to be that the only two categories of shit hit the fan (SHTF) scenarios that should be “prepped” for would those whose occurrence is [least likely, yet very severe, and those that are most likely, yet not severe](#), or at least, mildly to moderately harmful. He elaborates on this by saying that due to [the outlier fallacy](#), the focus of most preppers lies squarely upon the SHTF category of least likely, yet very severe, usually at the expense of prepping for the other category of most likely, yet not severe. Again, this would seem to reinforce what both Dobelli and Schneier have separately argued, in the sense that the [existential risk](#) of highly improbable events appears to have taken precedence over that of more likely threats.

So, the pertinent question then becomes, should probabilities dictate priorities? [As I've mentioned before](#), **the answer to security theater is security culture**, and an indispensable element of security culture is threat modeling and risk analysis. Given that the news cycle skews risk analysis, threat modeling becomes just as vulnerable as well; since this is indeed the case, it would explain why facts, statistics, and data take a back seat to fanciful stories of Armageddon. Despite the various and often conflicting tales being spun regarding the apocalypse, there are individuals who believe probability should *never* dictate priority; my question to them, then, is what should dictate priorities, instead? Subjective nightmares? Non-falsifiable “[precognitive](#)” visions? Good old-fashioned bigotry and prejudice?

You might be wondering, at this point, what threat modeling and risk analysis even are, since they are rarely mentioned within the alternative media. According to the Electronic Frontier Foundation's Surveillance Self-Defense project, [threat models](#) and [risk analysis](#) are defined, respectively, as:

*“A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called **threat modeling**. Once you have a **threat model**, you can conduct a **risk analysis**.”*

*“In computer security, risk analysis is calculating the chance that threats might succeed, so you know how much effort to spend defending against them. There may be many different ways that you might lose control or access to your data, but some of them are less likely than others. Assessing **risk** means deciding which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about.”*

Obviously, these concepts are borrowed from the field of computer security, however, I think they can be made directly applicable to all sorts of disaster scenarios in order to gauge the realistic probability of these worst case scenarios actually coming to pass. Applying the scientific method to SHTF scenarios, the worst of which might also be referred to as The End of the World As We Know It (TEOTWAWKI), is seldom done, for reasons that will become apparent later on.

[Doom porn](#), for all intents and purposes, are sensationalized guesses about how TEOTWAWKI will eventually occur; it is defined by the [Urban Dictionary](#) as:

“Articles or videos online (prevalently in the blogosphere) that mainly talk about the collapse of either the financial world or the world in its entirety. People can develop a fascination/addiction reading this stuff (much like people who watch regular porn).”

In other words, doom porn is applied [conspiracism](#). Once conspiracists lay off fretting about the details of, admittedly, violently suspicious events, such as the [9/11 attacks](#) or [Sandy Hook](#), then the most practical they ever seem to become is “preparing” for TEOTWAWKI, because they appear to have a deep seated, almost nihilistic wish for everything to just end. Conspiracism, and doom porn specifically, are greatly influenced by the news cycle, which, as a matter of course, throws intuitive feelings and rational models of security completely out of line with reality, while also increasing learned helplessness by encouraging its adherents to commit the outlier fallacy.

I would like to present, for your delectation, a handful of SHTF & TEOTWAWKI scenarios, whose very narratives strain [credulity](#). They are presented here, not with the intention of ridiculing anyone who sincerely and genuinely believes that these scenarios could, or will, come to pass, but rather, with the intention of stressing the importance of [homeschooling](#) over that of speculation, gossip, and conjecture – even for adults.

Seattle’s “Overdue” Earthquake/Tsunami Combo Pack

Kathryn Schulz’s [article in *The New Yorker*](#) last July claimed that Seattle will slide into the Pacific Ocean because of a tsunami caused by an earthquake resulting from the Juan de Fuca tectonic plate colliding with the North American plate. Exacerbating this is the quoted statement by the Federal Emergency Management Agency (FEMA) Region X director Kenneth Murphy, who said:

“Our operating assumption is that everything west of Interstate 5 will be toast.”

FEMA estimated that about a million buildings throughout the Northwest will either collapse or become compromised due to this earthquake, which is only considered “[overdue](#)” because of an estimated average that an earthquake in this region occurs in a 243 year cycle, and that considering it’s been 315 years since the last one, then therefore Seattle should be destroyed by a tsunami any day now. Add in the fact that the Pacific Northwest has no early detection system for tsunamis and earthquakes, mix it with the fanciful imagery of a 700 foot liquid wall containing a five-story assortment of “[pickup trucks and doorframes and cinder blocks and fishing boats and utility poles](#)” heading right towards the west coast in about 15 minutes from onset of the first shake, and you have a concoction for mindless panic and consumerist hysteria for prepackaged disaster kits.

Seismologist John Vidale was asked on Reddit about the realistic probability of this “overdue” earthquake actually demolishing part of the west coast, and Seattle in particular. Eric Holthaus’s [article in Slate](#) tackled the accuracy of this doomsday scenario by summarizing Vidale’s answers:

“Vidale said that the chances of the worst-case scenario happening in your lifetime, if you’re planning on living another 50 years or so, is [about 15 percent](#). That’s probably a better way of looking at the recurrence statistics than on an annual basis. Historically, the frequency of major earthquakes in the region is about [one every 300 years](#), which means we’re overdue for a megaquake if you average the past 10,000 years of Northwest geology. But the spacing between past magnitude-9 quakes was between 200 and 900 years. If the fault system maintains that pattern, the next big one could happen again tomorrow or in the year 2600. There’s no way to know.”

Obviously, this would suggest that the “overdue” earthquake/tsunami disaster would fit squarely into Eric English’s typology as being least likely, yet very severe. If Mr. English’s previously mentioned contention is true, then all of this concern about Seattle’s “overdue” earthquake suffers from [the sin of misplaced emphasis](#). To add insult to injury, Holthaus reported that Schulz engaged in “poetic license” in describing the magnitude of the entire affair. Not only that, but Holthaus further mentioned that the risk to Seattle was insignificant because that city is protected by the Olympic Peninsula and Puget Sound; Portland was similarly protected by both its 100 mile distance from the coast, but more importantly, the Columbia River as a natural barrier. Misleading statistics, much?

As a corollary example, the Geological Society of America published a scientific white paper this past August entitled, “[Pleistocene Relative Sea Levels in the Chesapeake Bay Region and Their Implications for the Next Century](#),” which posits that Washington, D.C. might be deluged by rising sea levels [due to global warming](#). Although I do have some empathy for those living right outside that den of inequity on the Potomac, would anybody with a conscience really miss the imperial city of the federal government? Ever since Adam Kokesh’s house was raided by government police for [loading a shotgun at the \(Orwellian titled\) “Freedom Plaza](#),” it’s just sad for me to read about how these scientists are fretting about how to save and preserve the headquarters of Leviathan.

Needless to say, “[natural](#)” disasters, whether they be in the form of rising sea levels or earthquake/tsunami packages, are noticeably hyped up by the corporate media for their own sensationalistic reasons, besides the fact that it increases the opportunity costs for their respective audiences, at least in terms of restoring or securing their own liberty. Whipping people up into irrational hysterics virtually guarantees their unquestioning obedience to whatever “[authority](#)” tells them to do, thereby perpetuating the [Hegelian Dialectic](#), regardless of whether the original “problem” was genuine or not.

The Interminable Economic Non-Collapse

Amongst all of the TEOTWAWKI scenarios, this one is, perhaps, the most convincing of the bunch. I must confess that over half a decade ago, I believed in what the doom-and-gloom-peddlers were spewing about bank runs, empty grocery store shelves, and worst of all, no [Internet](#)! Unfortunately, acolytes of the socio-economic collapse disaster scenario, in my experience, have typically been economically illiterate, since

whatever knowledge they've gleaned about economics has been limited to [Zero Hedge](#), the [Trends Journal](#), and worst of all, [The Economic Collapse Blog](#).

Speaking of the *Trends Journal*, I remember when Gerald Celente said the following on the [May 7th, 2010](#) broadcast of *The Alex Jones Show*:

*"The top trend: 'The Crash of 2010.' We stick with our forecast. Before the New Year begins, **no one** will be able to deny that the great equity markets have crashed. The currencies are being devalued around the world. Gold prices are well over \$1,500; we are still sticking with our forecast that the markets will crash before the year is out, and I also want to make this very clear: it's not only going to be a financial crash, it's going to come from a lot of different directions. Our greatest fear, and we said this when they began the great bailout bubble in March of 2009, is that when all else fails, they take you to war. So, our scenario is this, Alex – we're going to see 9/11 magnitude terror strikes happen. When they happen...the last time they happened after 2001, they closed Wall Street down for several days. If you had CDs, you couldn't cash them in (they are financial instruments). This time, they are going to close the banks, and when they reopen the banks, we forecast they will have devalued the dollar. So, they'll say, 'Don't worry about it, you'll be able to get your money out, it's backed by the FDIC, but you can't get it out all at once,' [yet] when you do get it out, it's not going to be worth a fraction of what it was before. So, these are the integrated systems that we are looking at, and I'm saying this so that people take proactive measures now. Don't wait to wake up one day, as you did yesterday, and see the markets collapse **around** you! Take proactive measures now, it doesn't cost **anything**, but if you don't plan for the worst now, and the worst happens, then you'll lose everything. If you take measures now, and things happen **slowly**, you haven't lost anything, you've gained."*

Jones, of course, lapped this up like nothing else, as is his way, by nearly salivating over the possibility of an economic collapse deteriorating into a "[Road Warrior](#)" situation. Fast forward over five years later to [August 8th of 2015](#), when Celente told Eric King the following:

*"I got it wrong, when I believed, that following the panic of '08 we'd have the big collapse in 2010. I had no idea that they would invent a thing called quantitative easing. I had no idea that they would keep 0% interest rates as a matter of policy that still exists **today**, and as your listeners well know, this free money that they've been pumping into this system, whether it's in China, whether it's in Japan, or the European Union, is what has kept the equity markets floating high, with the stock buybacks and the mergers and acquisitions, everyone knows the facts; however, I'm ready to forecast now, that between now and the end of this year, the end of 2015, we are going to have panic on Wall Street. There's going to be panic on the streets, more than Wall Street: the bottom has fallen out. They're only keeping Ponzi alive with this monetary methadone that's no longer able to fix his habit. What's going on in China is a global disgrace the way they are rigging the markets, and we heard from the IMF chief, Christine Lagarde, that she's basically in favor of China rigging*

the markets, as she is, with the U.S., the European Union and what they're going to it, and [unknown] in Japan, and all the rest, but it's running out of steam...[t]his is global. It's going to hit the equity markets, there's going to be panic on the streets. Eric, you are going to see a global stock market crash by the end of the year. It's not only going to be the [Dow](#), it's going to be the [DAX](#), [unknown], the [Shanghai](#), [Nikkei](#), there's going to be panic on the streets. From Wall Street to Shanghai, from the U.K. down to Brazil, you're gonna see one market after another begin to collapse. "

So, let me get this straight – Celente admitted to King that he was wrong about what he told Jones' listeners five years earlier (and everybody else at the time), yet I find it rather telling that he didn't know the Federal Reserve would coin the term "quantitative easing," despite the fact that [Stewart Dougherty mentioned quantitative easing by name in his article published on May 15th of 2010 at LRC](#), a mere week after Celente's interview with Jones. Perhaps if Celente had familiarized himself with the Austrian school of economics, he would've understood that, according to [Austrian business cycle theory](#), malinvestment is caused by an expansion of credit during the boom phase, which sows the seeds for the bust phase during the inevitable credit crunch.

Vloggers such as [BrotherJohnF](#), [SGTbull](#), and [Chris Duane](#) typically advocate [silver stacking](#) as the best hedge against inflation, despite the fact that [JPMorganChase has attempted to corner the market on silver bullion over the past few years](#). Any doubts about the viability of silver stacking, not to be used as sound money, but rather as just a hedge to be converted back into Federal Reserve Notes (FRNs) once the spot price is high enough, has been propagandized away by the production of "miniature documentaries" (aka, "mini-docs") such as [The Madness of a Lost Society](#) trilogy, which spells apocalyptic disaster for all, **but**, for the "relatively low" investment of thousands, nay, tens or even hundreds of thousand of dollars, you too can join the ranks of those who have become the "[awakened](#)" by buying up all the disaster supplies you'd ever need to throw into a closet and forget about since you'd never intended to use them, anyway. The whole exercise was one of security theater to make you **feel** safer without actually improving your security in any real way.

Total economic collapse does not make any sense whatsoever, especially if you view it from the perspective of the central bankers. Remember, [fractional reserve lending](#) necessarily requires the federal government, as well as individual borrowers (such as those who take out a home mortgage from a commercial bank), to ceaselessly borrow FRNs into the money supply in order to perpetuate never ending "economic growth." As such, there is interest attached to the principal being borrowed, but this burgeoning "national debt" can never be paid back, of course, and that's the point. In this authoritarian nightmare, **money is debt**, and for the central bankers to deliberately tank the economy into societal collapse would be [to kill the goose who laid the golden egg](#).

But wait! Wouldn't it be possible for the central bankers to *inadvertently* kill the goose (that is the free market) just through sheer recklessness, especially considering [Argentina](#) and [Zimbabwe](#) last decade? You must keep in mind that the Fed, as a central bank, is older than most central banks (except the [Bank of England](#)). They know all the tricks, and they know how to play the angles with their asset purchases, simply because they've been doing it longer than most. I'm not saying the Fed is invincible or otherwise immune to the laws of economics, but rather, these central planners *need* "the economy" to operate in order for [the State](#) to parasitically feed off of [the Market](#), and a [hyperinflationary depression](#), or even "just" a [currency war](#), interferes with that "business as usual."

[Downward class migration](#) is likely to be the most accurate explanation of what the doom porn aficionados

misleading describe as an economic collapse. Simply put, Jack Spirko's thesis is that due to the [government failure](#) that is central banking, most of the population on the socio-economic scale moves down a notch; the upper middle class become the lower middle class, the lower middle class become the working poor, the working poor become totally destitute, and so forth. Considering that the bankers are magicians, nobody who is even slightly knowledgeable about the evils of central banking should be surprised with, for example, the Fed's stubborn refusal to raise interest rates since 2008. In light of the fact that the Federal Open Market Committee (FOMC) has [repeatedly stated](#) that they intend to keep the interest rates artificially suppressed in order to "manage inflation" at a steady pace of 2% a year, in part to "stimulate" higher employment, is, quite frankly, laughably hysterical. The result of the FOMC's actions does little else other than incentivize [malinvestment](#), which repeats the business cycle once again.

Hyperinflationary depressions give us the best window as to how living conditions would deteriorate during a socio-economic collapse, but it would not become a TEOTWAWKI post-apocalyptic dystopia by any means. I say this because the total number of hyperinflationary depressions in recorded history took place over the course of two centuries. If the ratio of hyperinflationary events to the overall length of time from when the earliest began to when the latest one ended was measured, this could reveal something enlightening.

Therefore, in light of the fact that Wikipedia lists [12 hyperinflationary events occurring over a time span of 213 years](#), I calculate that the probability of hyperinflation occurring anywhere in the modern world to be a 1 in 18 chance; however, if I only calculate the probability of a hyperinflationary depression occurring here in America, then based on the hyperinflation from [the Continentals during the Revolutionary War and the Confederate dollars during the War Between the States](#), then the probability of an "economic collapse" in America would be a 1 in 114 chance, based on [the United States' historical longevity](#). This latter result would fit more comfortably into the "not likely, but very severe," category of Eric English's typology.

What might be the result of all this centrally "[planned](#)" economic turmoil? The further centralization of power into the iron fists of the State, of course. Leviathan has no wealth, so any pretense of money it has it had to inflate, borrow, or tax from the productivity of the hapless democratic citizenry. Inflation destroys the capital saved from the past, taxation robs from the fruit of one's labor in the present, and borrowing enables deficit spending whose bill is footed upon the backs of the unborn. Whenever the central planners hit a snag, they can just prod the executive branch of the federal government to launch [an unconstitutional war](#), which serves two purposes, namely, to distract the public from the seriousness that is intergenerational theft, and more importantly, to steal from the resources of foreigners who have caused us no harm in order to prop up fledgling equity markets.

Electromagnetic Pulse: Solar Flares or Thermonuclear Warfare?

Ever since the publication of novels such as [One Second After](#) and the airing of television shows like [Revolution](#), there has been a growing popular concern about the electrical power grid becoming suddenly inoperable, especially by way of an electromagnetic pulse (EMP). Whether it be due to natural phenomena or human attacks, EMP occurrences would definitely count as a TEOTWAWKI scenario, simply due to the sheer severity that a forcible take-down of the power grid would affect the business of everyday American life. Scientific facts and government documents, however, reveal quite a bit of detail that undercuts the assumptions promulgated by mass media.

Solar flares and coronal mass ejections (CME) are natural phenomena emanating from the Sun. These flares are sudden bright flashes, which are often accompanied by massive bursts of gas and magnetized fields from the solar corona. The [1859 Carrington event](#) directly hit the planet, causing telegraphs to fail, sometimes resulting in electric shocks to those operators. CMEs are a regularly occurring facet of nature,

because they can happen anywhere between [one CME every 5 days](#) to [three CMEs every single day](#), depending on the frequency of solar activity.

The [North American Electric Reliability Corporation](#) (NERC) released two reports that I think are demonstrative of the baseless hysteria that seeks to divorce one's feelings and models of security from the objective reality of security. NERC's 2012 [Effects of Geomagnetic Disturbances on the Bulk Power System](#) white paper reported in the executive summary that:

"The highly complex, interconnected North American power grid has provided a long record of reliable, secure delivery of electric power. However, solar storm or geomagnetic disturbance (GMD) events have demonstrated their ability to disrupt the normal operations of the power grid. The most recent example in North America occurred in March 1989, when a GMD led to the collapse of the Hydro-Québec system, leaving more than six million people without power for nine hours."

Notice that in an admitted "collapse" of a specific power grid, those 6,000,000 people had to go without electricity for only 3/8ths of a single day. Referenced inside this white paper was an earlier NERC report that was co-authored with the United States Department of Energy (DOE) in 2010 entitled [High-Impact, Low-Frequency Event Risk to the North American Bulk Power System](#), which stated in its introduction that:

*"While **some of these events have never occurred** and **the probability of future occurrence and impact is difficult to measure**, government and industry are working to evaluate and, where necessary, enhance current planning and operating practices to address these risks in a systematic and comprehensive fashion." [emphasis added]*

Whoa, hold on there for a moment – did DOE just admit that the probability of **rare** events that could negatively affect the North American electric grid, including "extreme solar weather," are, at best, tough to calculate? As if that wasn't bad enough, consider this sentence from the joint DOE/NERC report:

*"We will need the support of all of our readers to realize the vision of this effort: effective **public/private partnership** to address HILF [High-Impact, Low-Frequency] risks in a coordinated, systematic fashion." [emphasis added]*

Ah, there you have it – an abusive use of the [precautionary principle](#) by bureaucrats as an opportunity for a power grab. Why, may I ask, would these benevolent rulers want to encourage the development of even

more fascism? In any case, I guess it's refreshing to see the federal government and their "private partners" give an official sounding title to Eric English's "not very likely, but very severe" category.

Speaking of fascism, I think it's important to understand the nature of the relationship between NERC and the federal government. The [Federal Energy Regulatory Commission](#) (FERC) is an [administrative agency](#) ordered by the Congress to "remedy" the effects of the [2003 Northeast blackout](#) through the [Energy Policy Act of 2005](#), which "authorizes" FERC to designate a non-governmental organization who would be subcontracted out to enforce regulatory policy with FERC playing an oversight role. This corporatist relationship between NERC and FERC was established because in case anything went wrong, NERC would serve as, quite literally, the designated fall guy, while FERC could rush in and proclaim itself our savior. According to [Dr. Peter Pry's testimony before FERC](#) regarding the previously mentioned 2012 NERC report:

"We urge the NERC Report's authors to recognize that their report, unique among all others in its optimistic assertions, could contribute to a possible failure to harden the U.S. grid against a severe geomagnetic storm. The electric grid alone is not at risk. Everything in our modern society depends, directly or indirectly, upon electricity, including all the other critical infrastructures—communications, transportation, banking and finance, food and water—that sustain modern civilization and the lives of 300 million Americans. If a great geomagnetic storm proves to be catastrophic, as all previous U.S. Government studies have warned would be the case, then NERC could be responsible for contributing to an unprecedented national catastrophe."

Dr. Pry, as the executive director of the task force on national and homeland security, goes onto slyly suggest that the electric grid become **nationalized** in order to protect American electricity from either a natural or artificial EMP. This use of the Hegelian Dialectic, combined with horribly asinine fiction like [One Second After](#), essentially promotes centrally planned socialism as the solution to the fascism they themselves legislated in the first place.

Pursuant to [an act of Congress](#), the federal government established the [Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack](#) (the EMP Commission), which found that there is "critical infrastructure" that presented a "national security vulnerability," from the high-altitude detonation of a nuclear weapon. Dr. William Graham, chairman of the EMP Commission, said in his [2008 congressional testimony before the House Armed Services Committee](#) that:

"Several potential adversaries have the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse, and others appear to be pursuing efforts to obtain that capability. A determined adversary can achieve an EMP attack capability without having a high level of sophistication. For example, an adversary would not have to have long-range ballistic missiles to conduct an EMP attack against the United States. Such an attack could be launched from a freighter off the U.S. coast using a short- or medium-range missile to loft a nuclear warhead to high-altitude. Terrorists sponsored by a rogue state could attempt to execute such an attack without revealing the

identity of the perpetrators. Iran, the world's leading sponsor of international terrorism, has practiced launching a mobile ballistic missile from a vessel in the Caspian Sea. Iran has also tested high-altitude explosions of the Shahab-III, a test mode consistent with EMP attack, and described the tests as successful. Iranian military writings explicitly discuss a nuclear EMP attack that would gravely harm the United States. While the Commission does not know the intention of Iran in conducting these activities, we are disturbed by the capability that emerges when we connect the dots."

Besides the fact that [Ed Snowden](#) would probably like to take Dr. Graham to task for using [misleading analogies for intelligence collection](#), what cannot be ignored is Dr. Graham's not-so-subtle saber-rattling against the Ayatollah's theocratic government. Might it be possible that all of the mainstream media's [interviews and simulated depictions of how an EMP attack could occur](#) is thinly veiled neo-conservative propaganda, which advocates for preemptive thermonuclear warfare against the Iranians?

Of course, the real crisis is not a future EMP attack, but rather the monopolization of the electrical grid itself. Sure, one could point out that the [Texas Interconnection](#) is proof that there is no such monopoly, but what they fail to realize is that the Texas Interconnection fails under the auspices of NERC, and by extension, FERC's "rulemaking" authority. [Privatization](#), **not** corporatization, would have averted this problem right out of the gate, but unfortunately, most people are economically illiterate, which would explain why central planning is so ubiquitous to the government's own emergency preparations, especially considering they created the vulnerable "interdependent" infrastructure in the first place.

What is the probability of either a direct CME hit or a nuclear EMP attack disrupting the electrical grid and plunging Americans into a total blackout? According to a workshop report by the National Academies Press entitled, [Severe Space Weather Events: Understanding Societal and Economic Impacts](#), it says:

*"A widely accepted approach to **risk analysis** involves estimating event probabilities and then making estimates of event consequences. It was noted, though, that in complex systems characterized by strong interdependencies, it is very difficult to identify all impacts from a large-scale disruption, let alone to quantify their physical and financial consequences." [emphasis added]*

In other words, calculating the probability of these disruptive events is virtually impossible to do so accurately. Consider also, that a CME hit is more of a global concern, whereas a nuclear EMP attack is mainly limited to the North American continent. Keep in mind too that as I read the copious literature on both CMEs and nuclear EMPs, that these "experts" kept repeating that they have little in the way of "historical experience," and that much of what they are postulating is based, at most, upon **computer simulations**, in much the same way [the National Institute of Standards and Technology determined how the collapse of World Trade Center Building 7 occurred](#) without being hit by an airplane on 9/11.

Guessing as to the likelihood of a CME event produces wildly dissimilar results, as you can imagine. The [National Oceanic and Atmospheric Administration](#) (NOAA) is "predicting" that [solar flares have a 80% chance of impacting Earth today](#), yet there is also a reference to a indie movie trilogy promoted by the

same author; the only original source I was able to find was this NASA press release from May of 2013 that said they discovered [three X-class flares within 24 hours](#). Probably a more realistic guess would be [a 1 in 8 chance by 2020](#), which itself is based upon [a 12% success rate by 2024](#), according to physicist Pete Riley.

Needless to say, I disagree with these guesses for at least two reasons. First, the [Earth's orbit](#) keeps the planet a constantly moving target from the Sun's CMEs, which are shooting blindly since they are not consciously being aimed; as [Dr. Michio Kaku](#) has explained, [although there have been CMEs that have grazed Earth's orbit](#), the chances of a direct hit are pretty slim, arguably lower than [random chance](#). Second, even if Pete Riley's estimates were objectively correct, the other side of the coin is that there would also be an 88% chance there **wouldn't** be a direct CME hit by 2024, and by extension, a 7 in 8 chance a direct CME hit would be avoided by 2020.

Regarding the probability of a nuclear EMP attack, think about the fact that, aside from nuclear test explosions, atomic weapons have only be used in warfare exactly **twice**: [Hiroshima and Nagasaki](#). The horror of what the Japanese suffered greatly encouraged other nation-states to tread carefully on the use of their nuclear stockpiles, particularly with regards to nuclear proliferation, even accidentally. Effective military strategies like [mutually assured destruction](#) incentivized even the most soulless, war-mongering politicians to avoid creating their own [nuclear holocaust](#) if for no other reason than for the sake of maintaining their grip on absolute power.

What lessons can be learned from these overly hyped CME/EMP TEOTWAWKI scenarios? Decentrally privatize the production of electricity so it would be unnecessary in the future to patchwork together Band-Aids if a security concern arises, stop fretting about things that probably won't happen, and if they do, your earlier actions in hardening the infrastructure is the best you can do anyway. Most importantly, central planning never, ever, works when it comes to economics, and [it will never work for emergency preparedness either](#); having plans by the many, and not by the few, will greatly aid in not only survival, but also increasing the quality of life right now. Manipulatively using the precautionary principle on the grounds that a CME or nuclear EMP will cause an electrical blackout since they are "existential threats" seems little different to me than when Henry Paulson demanded ([or would that be threatened?](#)) Congress to hand out bailouts for Wall Street bankers on the non-existent justification that [the free market is an "existential threat" to stock-brokers and derivatives traders](#).

I doubt this will win me a ton of friends, but it needs to be said – what concerns me more than this nonsensical drivel about TEOTWAWKI being caused by a CME/EMP type event is this recurring diatribe about how the Iranian theocrats will, allegedly, be the ones most likely to launch such an EMP attack against America. This presumption that these Muslims will kick off the apocalypse seems to thinly justify the use of a [pre-emptive nuclear strike](#), which if accomplished, would more likely kick off [World War III](#) instead. I don't know about the rest of you, but the last thing Americans need is another unconstitutional war to embroil themselves in.

American Islamism: "Stealth Jihad" to Impose Sharia Jurisprudence

Over the past several years, the [American patriot faction](#) has expressed concern about what they consider to be a plot by naturalized and native-born Muslims to wage a ["stealth jihad"](#) in order to establish a caliphate within the United States that would impose Sharia law, thereby subverting and overthrowing the 1787 federal Constitution. According to proponents of this claim, like [Brigitte Gabriel](#), this is why the violently suspicious events involving Muslim perpetrators, such as those in [Garland, Tex.](#) and [Chattanooga, Tenn.](#), happened at all – these Muslim jihadists decided to go hot, as it were, because ["they hate us for our freedoms,"](#) or so we are told. This belated attempt to revive the legitimacy of the [terror war](#)

is patently ridiculous at best, and exceedingly dangerous at worst.

Right off the bat, I think it's essential to remind everyone of the United States federal government's foreign policy towards [Islamism](#) for the past several decades. [Between 1979 – 1989](#), the Central Intelligence Agency (CIA) armed and financed the *mujahideen* as the primary mission of [Operation Cyclone](#). Following the withdrawal of the Soviet Union from Afghanistan, the surviving *mujahideen* were betrayed by the CIA once they had outlived their usefulness to them and were subsequently relabeled “Al-Qaeda,” a label that later served its purpose as the convenient boogeyman responsible for the 9/11 attacks, which itself was the result of [blowback](#). Once the Iraqi “insurgency” had been greatly quelled, the surviving “Al-Qaeda in Iraq” Islamists [regrouped by joining up with the so-called Syrian Free Army in 2011](#), which soon after coalesced into the Islamic State of Iraq and Syria (ISIS). Three months ago, [Dan Sanchez wrote](#):

“Given all this, you would think right-wing nationalists would be alert to and aghast at abundant reports that their own government has knowingly supported Islamic extremists in Syria (and elsewhere), including al-Qaeda, the very group responsible for 9/11; especially since that support led to the rise of ISIS (formerly al-Qaeda in Iraq, or AQI) and that such a treasonous policy has long occurred under ‘crypto-Muslim’ Barack Hussein Obama. But, oddly enough, they’ve given Obama a pass on this. Why hasn’t Fox News been blasting alerts like ‘Obama Backs Muslim Terrorists, Helping to Create the Islamic State’ for years? Wouldn’t their xenophobic viewers gobble up such red meat with relish? Couldn’t the Republicans make stacks of political hay with such a talking point? But, no, apparently bigotry and scaremongering are only to be harnessed to support war, and never to oppose it.”

In much of the same way that serious martial arts disciplines have a traceable lineage from sensei to apprentice, ISIS is descended from the Afghan *mujahideen*, who might as well be disgruntled ex-employees of the federal government.

I remember how those of Arabic ancestry were treated after 9/11. They were frequently [unjustly profiled](#) at the airport, and commonly reviled by those who had been suckered in by the sophistry of the neo-conservatives like [William Kristol](#). Much like those **Americans** of German ancestry during World War I, as well as those **Americans** of Japanese ancestry during World War II, the **Americans** of Arabic ancestry during this “War on Terror” were targeted by the federal government, including the ones who weren’t even Muslims, such as the [Coptic Christians](#). Equal opportunity oppression, much?

Semantics are very much in play here as well, especially in light of the so-called “moderate” versus “radical” Muslims. Gary Hunt has explained the difficulty in distinguishing between these two descriptors, based upon what [Fahah Ullah Quereshi said to the Sunnis in Scandinavia](#) last year. Might I suggest an alternative that’s a tad bit more accurate – perhaps Muslims versus Islamists? It’s one thing to worship in accordance with one’s faith, but once that faith has transgressed across [the wall of separation between church and state](#), then it’s time to stamp out the emerging theocracy before it can entrench itself within the government, and that very constitutional guideline applies not only to **political** Islam (that is, [Islamism](#)), but also those who promote the erroneous notion that “America is a Christian nation,” despite [Article 11 of the 1796 Treaty of Tripoli](#):

*“As the government of the United States of America is **not in any sense founded on the Christian Religion**, – as it has in itself **no character of enmity against the laws, religion or tranquility of Musselmen**, – and as the said States **never have entered into any war or act of hostility against any Mehomitan nation**, it is declared by the parties that no pretext arising from the religious opinions shall ever produce an interruption of the harmony existing between the two countries.” [emphasis added]*

I'll remind the American patriot faction that in order for them to be consistent with the original intent of the Founders in upholding constitutional republicanism, they ought to follow the tradition of religious toleration as set forth by [Sir Thomas Browne](#) if they truly value religious liberty, instead of pandering to special interests run by manipulative clergy who seek to use the monopoly power of [the State](#) as their own personal [billy club](#). Back in 2011, [Cathy Young](#) wrote:

*“The push for Shariah bans is puzzling, to say the least. Since Muslims make up about 1 percent of the U.S. population, and government establishment of religion is prohibited by the Constitution, **a Shariah takeover in America is about as likely as a zombie apocalypse**. Yet to proponents, this is a threat that must be stopped while there's still time. A closer look at the purported evidence for 'creeping Shariah,' however, shows a lot of **skewed and garbled facts**—and issues by no means unique to Muslims or Islam.” [emphasis added]*

The fact of the matter is that American Christians have more political clout with the enemy rebel government than American Muslims ever had, and I think they will continue to do so for the foreseeable future; **that** is the reason why I've said before that [Islam is not the problem](#).

Who would stand to gain from demonizing religiously devout American Muslims as being equivalent to the Islamists (that is, **political** Islam) using the very same [guilt by association technique that the Southern Poverty Law Center used against American patriots](#)? The [Clarion Project](#) has released a number of hit pieces that were produced, funded, and even written by a Canadian-Israeli dual citizen, [Rabbi Raphael Shore](#). In terms of answering the infamous *Cui bono?* question, it would seem to be the case that this hostile foreigner wants the American federal government to wage proxy wars against Muslim countries on behalf of Israel, which seems to coincide nicely with General Wesley Clark's exposing of the “Defense” Department's plan to [topple seven countries in five years](#), starting with Iraq and then Syria, Lebanon, Libya, Somalia, the Sudan, and “finishing off” Iran, thereby exponentially increasing the risk of thermonuclear warfare. Apocalyptic death-wish, much?

What frustrates me more than anything about this TEOTWAWKI scenario is that it completely ignores or misrepresents the anti-Islamist Muslims. [Maryam Rajavi](#) and the [Iranian Resistance](#) have steadfastly held that a separation of church and state is their answer to the Ayatollah's theocracy, which debunks the entire notion of an Islamic “global jihad” by itself. “*Madrasa*” is just the Arabic term for school, and does not connote some sort of uniquely Islamist brainwashing propaganda mill, unlike [American government schools](#). Ironically, [the vast majority of terroristic related deaths are Muslims themselves](#), especially considering that [Western wars have killed 4,000,000 Muslims since 1990](#). Where exactly is this

“Islamization” happening in the United States, other than those cherry-picked locations like in Dearborn, Mich., in light of the fact that only 7 – 15% of the American population is Muslim , as opposed to 76.5% being Christian?

The history of empires automatically debunks a global caliphate, because once empires get too large, they lose control and collapse, every single time, without fail. I suspect part of the reason none of the American patriots have taken up my proposed business model for handling those Mexican nationals who trespass across the Rio Grande is because they’d rather guard military recruitment centers instead, despite the Posse Comitatus Act of 1878; why bother protecting private property for profit when it’s so much more acceptable to guard government property for free? Sensationalism, first and foremost, is what drives this virtually non-existent threat of an Islamist “takeover” of America, and notice also that this mindless fear is being driven primarily by the news cycle and the terror-industrial complex.

What is the probability of Islamists violently overthrowing the federal government and enforcing Sharia law, thereby subverting the U.S. Constitution? If the Islamists can survive a 24/7 rolling gun battle with the Chicago Police Department over the course of a week, then they might have a slim chance of victory; absent that, I’m going to go ahead and assume that their chances of establishing an American caliphate are about as successful as the Banzhaf power index for each Illinoisan voter actually determining the results of a government election. To paraphrase St. Paul, it is time to put away childish things.

Eschatology & the Intellectual Dishonesty of Lifeboat “Ethics”

Predications about when TEOTWAWKI will happen have *a/ways* been incorrect, without exception, and the proof of this lies in the fact that you and I are still here and enjoy the quality of life that we do. Harold Camping’s proclamation that “the Rapture” would occur on May 21st of 2011 turned out to be the failure that the atheists correctly presumed it would become. Given the historical precedent for mass hysteria, even from admittedly fictional TEOTWAWKI scenarios, like Orson Welles’ *War of the Worlds*, when will people learn to become more skeptical of these outlandish speculations and unfounded conjectures about the so-called “end times?”

Eschatology is a theological sub-field that focuses on the study of how TEOTWAWKI might occur. Believe it or not, there are tales that have been spun in Abrahamic religious texts that describe TEOTWAWKI in excruciating detail, which interestingly enough, tend to mimic each other. Christian eschatologists believe in a 7 year long “tribulation” period ruled by an “antichrist” who will be eventually defeated by Jesus of Nazareth and who will then, ironically, rule here on Earth for a millennia; Muslim eschatologists similarly describe that Isa (Jesus) will assist the Mahdi to engage in a “final battle” against Mashi ad-Dajjal (the “antichrist”), which afterwards the General/Last Judgment will take place of all humanity by Allah/Yahweh.

My irreligious spirituality might be termed, “deistic apatheism,” by which I mean that I think the universe was created and then naturally evolved on its own without any supernatural interference from that point forward, **but** I don’t think whether other humans share this position will encourage them to fundamentally alter their behavior for either the better or worse, so it’s not worth mentioning publicly at any real length, quite frankly. I mention it here, though, to explain why I take a pretty dim view of theology, and eschatology specifically, because it’s all based on revealed religion, which itself relies on a trifecta of clergy, designated buildings, and “holy books” that are used to perpetuate confidence tricks against highly gullible people out of their hard earned wealth. In a somewhat similar vein, Montagraph’s vlog about the projected collision of Nibiru with Earth this upcoming September 23rd will certainly by October reveal that doom porn really does require quite a bit of blind religious devotion in order for its adherents to believe in it, despite whenever it proves to be blatantly in error once the predicated disaster fails to come to pass.

The pertinent question here, though, is whether eschatology is the source behind these wildly implausible and improbable TEOTWAWKI scenarios? I don't think so, because all of this speculative conjecture about TEOTWAWKI gave rise to eschatology, not the other way around. If I had to make an educated guess, it would be the irrational application of our [reptilian brains](#), which are hardwired for survival, to the real world that gave rise to doom porn.

An expression of this irrationality is the use of [lifeboat dilemmas](#) to either justify or delegitimize a range of beliefs, ideologies, and lifestyles. [Murray Rothbard and Ayn Rand both detested](#) the use of these so-called "lifeboat ethics" to trash libertarianism and Objectivism (respectively), because they were usually used by authoritarians of various stripes and flavors to prop up the "authority" of [the State](#). Unfortunately, "preppers" immensely enjoy positing lifeboat dilemmas as if it was going out of style; for instance, J.D. Dutra invented [Conflicted: The Survival Card Game](#), which is a [tabletop game](#) whereby you are presented with a hypothetical scenario and then you have three minutes to describe to all the other players how you would handle the situation. Preppers have been seriously using this game as a [vetting](#) tool to weed out potential undesirables from their retreat groups, and [Dutra even admitted that this was the original purpose behind his invention of the game](#). Needless to say, [David Kobler](#) should know better than to promote lifeboat hypothesizing as a form of gaming, especially considering not only that [hard cases make bad law](#), but also because of [the myth of the line in the sand](#).

Listen, even if it turned out that I was wrong about the previously mentioned TEOTWAWKI scenarios by having one of them actually occurring, that does not therefore mean doom porn would be proven correct or even legitimate, for that would be to succumb to the [non sequitur fallacy](#). A systematically recurring problem with doom porn is that it regularly commits different types of fallacious reasoning, and the cure for doom porn is [homeschooling](#), which usually teaches cogent reasoning at some point. The fact of the matter is lifeboat dilemmas are used to manipulate human emotions, thereby skewing one's feelings about security, which result in a mental detachment away from the objective nature of security, as Schneier pointed out.

Common Signs of Actual Disasters

Outside the imaginations of doom porn enthusiasts, disasters that actually occur tend to share characteristics, regardless of the specific emergency. Generally speaking, the features of a genuine SHTF emergency include at least some, if not most or even all of the following:

- No Internet and/or the phone lines are jammed or busy
- Empty grocery store shelves
- Bank runs and/or ATMs no longer work
- Empty gas station tanks
- Overrun hospitals
- Gridlocked roads
- No tap water
- No AM/FM radio wave broadcasts
- No electricity (aka, "grid down")

Should any combination of these signs come to pass and either happen very quickly one right after another or pop up one at a time over the course of, say, a week, then it's probably time to [get out of Dodge](#). The cause of whatever happened is only significant initially if it will help you survive; otherwise, just make your

decisions in order to keep living and then *maybe* you can begin figuring out what the hell happened, assuming you even care in the first place.

I'd like to address whether physical violence is a sign of a SHTF emergency. The survivalists I keep in touch with recommended to me, in preparation for this article, that I include things like frequent yelling, hysterical screaming, car crashes, road pileups, urban rioting, rampant killing, and gunfire and explosions as common features of actual disasters. I fail to see how physical violence of any kind is a key recurring feature of disasters **in general**, but rather, they seem to me to be more of a **secondary** set of features; for example, if there is no way to travel by car and buy food, then desperately scared people make careless mistakes and end up dead, or amorally opportunistic jackasses decide to rob and maybe even kill those who don't possess or know how to wield *liberty's teeth* in order to forcibly defend their own private property.

However, instead of dwelling on SHTF emergencies, I prefer to focus on self-sufficiency, because the only disaster worse than a sudden breakdown of the infrastructure is the continuation of our overall political situation. Self-sufficiency, including living off-grid in the here and now, is perhaps the strongest expression of a vote of no confidence in the established system as it stands. I, for one, do not "need" some ridiculous doom-and-gloom scenario by which to motivate me to separate myself from this decrepit cesspool that manifests itself as the raw power and lie of the moment, and I think I have amply demonstrated this already by *canceling my voter registration*. How many other people can honestly say the same?

Realistic SHTF Scenarios

If economic "collapse," Islamist caliphates, "overdue" earthquakes, and CMEs or nuclear EMPs knocking out the power grid are notorious examples of doom porn, then what would be realistic emergencies instead? Generally speaking, most realistic emergencies are only dangerous as they are because of the State's *coercive monopolies* on the provision of security and adjudication services, what constitutionalists refer to as the executive and judicial branches of government, respectively. Anytime you invite *central planning* into any human endeavor there is *government failure*, which is committed through a myriad of ways that has provided enough subject material to last the entire publishing careers of free market economists.

For the sake of brevity, it is the *American police state* that exacerbates or generates the conditions for realistic emergencies, aside from the weather and infrastructure breakdowns (such as trucker strikes). Consider the statistics of arrests made, the incarceration rate, *civilly forfeited property*, search warrants issued, *wiretapping orders granted*, home raids, traffic stops conducted, and *democide*, and then gauge the probability of whether you are going to spend a night in jail versus being killed by an Islamic jihadist, for example. Once you've done that, then come back and tell me that "*America is not a police state*" with a straight face, if you can.

Other realistic scenarios might involve computer difficulties or even betrayal. Any number of breakdowns or targeted hacking might compromise your data, and don't forget that it is common for *the government to nab people's computers during raids*. Fraudulent child support through *false parentage* as a result of infidelity, *demonization*, and particularly *snitching* have all been used to incur the wrath of the State through their police forces, especially in phony "domestic violence" or "kicked out of the house by an angry spouse" scenarios. *According to Laura Southern*, men are raped more often than women if you account for prison rape, men are almost half of all genuine domestic abuse victims, and men commit ~ 80% of all suicides. If these statistics are objectively true, then if those vile situations that Miss Southern mentioned don't count as SHTF scenarios, then I don't know what does, honestly.

The Necessity for Bugging Out & Alternative Shelters

Obviously, you can play the “what if-ing” game all day long, but what’s needed in order to just survive are realistic options for coming out the other side of a disaster at least half-way intact. If you already know [how to reduce ratios](#), you are well on your way towards calculating **for yourself** the probability of certain types of events happening or not happening, presuming your measurement assumptions are correct, of course. Should you require a refresher on [middle school](#) arithmetic, then be sure to read [my primer on homeschooling](#) for your educational options.

Go ahead and pretend that you are suddenly broke, impoverished, deeply indebted, or otherwise homeless, for whatever reason. **What are you going to do from that point onward?** Try answering the following list of questions:

- Would you have anyone to turn to for help?
- Are you capable of living on the street, if only temporarily?
- Could you survive the climate outside without electricity where you live for a week, or even for a weekend? If not, could you quickly travel to another part of the country where you can?
- Have you got an alternate place to sleep, whether that be a [travel-trailer](#), van, cave, tent, or anywhere at all?
- How would you communicate if your computer had been seized? Could the government police easily read your data? Would you have your backup files in a secure place?
- If you have children or elderly family living with you, how would you feed, clothe, and medically treat your dependents?

If you answered “no,” or worse, “I don’t know” to any of these questions, then consider those security vulnerabilities as guidelines to what you need to shore up on so you can have the confidence and peace of mind that no matter what situation may be foisted upon you, you have gotten your bases covered. As you can no doubt tell, I am encouraging you to formulate a bug out plan **ahead** of time for realistic SHTF scenarios, much like you ought to make [an arrest plan](#). Freedom is all about making your own choices, and **knowing** what your choices are, or creating them ahead of time, is what responsible adults do.

Don’t run around like a chicken with its head cut off, though – take your time and do it right. Whether it be caring for your dependents, constructing alternate shelters, opening a foreign bank account, securing your archived records, or burying supply caches, your actions in the present might just make the difference as to the quality of life you’ll enjoy in the future, if not also quite possibly your very survival, depending on the nature and severity of the emergency. What I do suggest, before you begin exploring these and other options, is to first perform some threat modeling and risk analysis, so you can realistically figure out what you’re probably going to be dealing with in the first place.

The Grandiosity of Conspiracism

[Security culture](#) is the application of espionage techniques towards increasing and maintaining an individual’s personal privacy. Threat modeling and risk analysis inherently threaten the integrity of conspiracists, because it exposes and debunks their most fervently held misconceptions of the world they live in. Historical revisionism and detailed investigative exposés provides original material for [institutional analysis](#), which is the antithesis, and the antidote, to conspiracism.

Conspiracism is, first and foremost, a hobby and a lifestyle simultaneously. Conspiracists derive their sense of self-worth from projecting their worst fears onto others. They are not interested in redressing their

grievances, but rather, they believe that the very act of proselytizing their grievances **IS** the remedy itself. Most conspiracists are [reformists](#), and since reformism is applied collectivism, this would imply that most conspiracists are, quite possibly, collectivists of some kind.

Doom porn is only possible because of conspiracism; doom porn is meant to be revealed in forever, for without it, conspiracists would quickly become empty hollowed-out shells of their former selves. It is because of conspiracism and the mindless sensationalism it breeds, is a large part of the reason why liberty has not been restored here in America in any sort of noticeably broad way. The news cycle generates conspiracism much like how the sun causes the chlorophyll in plants to engage in photosynthesis. [Mean world syndrome](#) infects the minds of die-hard conspiracists, and can even transfer to their non-conspiracist allies.

Science and logic are the enemies of conspiracism. Doom porn reinforces the [victim mentality](#), especially learned helplessness, primarily through information overload, which is usually delivered through such as rapid fire, emotionally charged hysteria that is difficult for the recipient to calmly evaluate and judge the information on its own merits in real time. Like the news cycle, doom porn reinforces confirmation bias.

More than quite a few people will likely feel greatly offended by this article, and my hope for their disillusionment from treating their survival as some sort of twisted [live action role-playing game](#) is **exactly** what I was aiming for. The probability of most TEOTWAWKI doom porn scenarios can't be calculated anyway, and even when they can be, the success ratios are so incredibly low that the more typically mundane yet dangerous things are what should be "prepped" for instead, assuming that probability dictates priorities. Regardless of a particular scenario, the signs of a genuine SHTF emergency, as well as what you *should* be doing to survive it, are more similar than not.

Too much of an emphasis has been upon potential future emergencies, and not enough on self-sufficiency and independence for **right now**, despite whatever atrocities the State commits *this* week. At the risk of sounding like a [pothead hippie](#), your actions should be motivated by your love of freedom, not by your dread of the apocalypse. Survivalism and security culture are firmly within the realm of [direct action](#), yet, I simply disapprove of how they've been applied up until now; instead of *acting* upon libertarian principles, they have been used, thus far, to supplant them.

If there is anything I'd like you all to take away from this examination into conspiracism, doom porn, threat modeling, and risk analysis, it would be this – **skepticism is healthy!** It will *always* be the end of the world, as we know it. And you know what? [I really do feel fine about it](#), because I am already free within my own mind. You can be too, provided that you commit yourself to rational discourse and scientific inquiry.

The Libertarian Case for Judicial Transparency

By: Shane Radliff & Kyle Rearden

February 8th, 2016

“It is the lawyers who run our civilization for us -- our governments, our business, our private lives. Most legislators are lawyers; they make our laws. Most presidents, governors, commissioners, along with their advisers and brain-trusters are lawyers; they administer our laws. All the judges are lawyers; they interpret and enforce our laws. There is no separation of powers where the lawyers are concerned. There is only a concentration of all government power -- in the lawyers. As the schoolboy put it, ours is a government of lawyers, not men.” - [Fred Rodell](#) [Emphasis added]



The [1787 United States Constitution](#) is fraught with [monopoly powers](#), one of them being the monopoly on [adjudication services](#). When it comes to that monopoly, competence, and efficiency, disappear in a cloud of smoke, replaced by injustice. The already uneven playing field appears much worse, when you take into account that the lawyers (both, the prosecution and the defense), judges, and the bureaucrats are all on the same team. Secrecy, cover-ups, and “[testilying](#)” are part of the court’s [modus operandi](#), hence, the importance for judicial transparency.

If you’ve visited the [Liberty Under Attack](#) website within the past six months or so, there’s a good chance you’ve seen the [political prisoners tab](#), which contains the court documents for a number of defendants, both accused and convicted of “victimless crimes.” We’ve realized that there has been no explanation of our reasoning for putting that archive together, so the time has come to offer one.

First, I will explain “why” judicial transparency is important, as well as provide some examples of terrible judicial transparency that I have come across, which has motivated me to continue expanding the archive. Secondly, [Kyle Rearden](#) will tell you “how” to provide judicial transparency, whether it be for yourself, or for someone else. He will also explain the archiving system that we have utilized, which is the best we have been able to come up with thus far.

Why Should Libertarians Care About Judicial Transparency?

About the same time the political prisoners archive was conceived, I was just beginning my [circuit of political field trips](#), which required me to read quite bit of Illinois law. One purpose for the political field trips, was to make the authoritarian activities of the local county government transparent to those who also happen to reside in Bloomington/Normal. That was the same time that I realized the importance of judicial transparency, which quickly led into the formulation of the aforementioned archive.

The initial political prisoners were particularly easy, as many of their cases had already been completed; these were, the Hutaree Militia, Darren Huff, Larry Myers, and Robert Beecher.

Then an old, now forgotten, darling of the patriot movement came to my attention. *Enter, [Charles Dyer](#)*.

When I first heard about his case, I was extremely motivated to obtain his court documents. That being said, judicial transparency was rather lax, as the only documents available were hosted on Scribd. There were a number of issues when it came to those documents. First off, there were only a handful of court documents available. Additionally, one of the documents in particular was missing a page. Lastly, some of the supposed “court documents” had just been transcribed into Microsoft Word documents, which removed all authenticity, thus making them absolutely useless for our purposes.

After I got everything useful off of Scribd, I contacted Dyer’s current girlfriend, Karyn Hardiman, and his mother, Janet Dyer. I was able to obtain a number of documents, but was unable to obtain the 3rd trial transcript, when he was convicted. After several months of fruitless back and forth with Hardiman, Dyer, and even a short exchange with none other than [Nancy Genovese](#), it became obvious to me that I was getting nowhere fast, so [I gave up on Dyer’s case](#).

That was my first encounter with the currently abhorrent practice of judicial transparency by “supporters” of these political prisoners, and it certainly left a deep impression upon me. With recalcitrant “supporters” like these, why worry about statism?

Another example is the [case of Dwight and Steven Hammond](#). The Bundy Ranch blog [posted a long exposé of their entire case](#), and of course, there was not a single court document available to verify the claims that they had made. To make matters worse, [Ammon Bundy](#) put up a YouTube video prior to the [occupation of the Malheur Wildlife Refuge](#), where he [showed a massive stack of court documents](#) on camera. I was able to obtain a handful of court documents from the Internet, but no thanks to a man who thinks God wanted him to [squat on a birdcage](#) in Oregon.

Then, a couple of weeks into the occupation of the refuge, Pete Santilli made the “[Hammond Legal Files](#)” available for download on his website. I immediately downloaded them and took a look. The first thing I noticed in the [682 page PDF](#), was that the bulk of the documents were just letters to and from the Bureau of Land Management, the U.S Fish and Wildlife Service, and other governmental agencies. The second thing I noticed is that the first and last page were both documents from 1998. I continued perusing, eventually realizing that they were not in chronological order. Now, I understand that they were probably in a rush to make them available,

so I'll give them a little leeway there, but come on! For people who are "professionals" because this is how they make their livelihood, why would I be considered an "amateur" when I do a better job without expecting a paycheck in return? Considering the unorganized order of the documents, there is literally no way to "connect the dots."

In summation, this was another encounter with lackadaisical judicial transparency, to say the least. Notice a pattern?

As you can see from the examples provided, there is a serious need for organized, easily accessible court documents. I can't tell you how many times I've listened to the callers of other alternative media broadcasts who express a desire for such a user-friendly archive. We have tried to fill that void, but there are only a few of us, and the number of political prisoners increases quite a bit, considering that [America is a police state](#).

So, why is there a necessity for judicial transparency?

First off, without knowing what the government is saying, there is no way for the defendant to mount a legal defense. In light of the aforementioned examples, it is possible that better judicial transparency could have assisted them in the execution of their litigation strategies. Obviously, that's not a guarantee, but it definitely wouldn't have hurt. Additionally, if the government is lying or doing something illegal, such as under "[color of law](#)", the way to discover (and prove) that is through the court documents. Lastly, consider the supporters of the various political prisoners. Without judicial transparency, they are essentially left in the dark, much like how Dyer's supporters were for years (and still are, mainly because the transcript for the third trial is being censored by his own relatives). Being able to keep updated with the case can give them peace of mind, and if anyone is independent media or freelance journalists, they might be able to assist in mounting a defense.

Briefly put, the whole point of judicial transparency is to:

1. Prove the existence of [political prisoners](#) within *these* United States, particularly as a symptom of the police state, and
2. Demonstrate the consequences of the failure to practice good [security culture](#), especially regarding the opportunity costs incurred by these political prisoners.

In summation, judicial transparency is *crucial* and the process of providing it is a skill everyone in the alternative media needs to learn. It's not a difficult task, although it does take a bit of work and time. It's not sensationalistic, but in this struggle for freedom, there are necessary mundane tasks; providing judicial transparency is certainly one of them.

How Can Libertarians Increase Judicial Transparency?

Now that you understand *why* judicial transparency is crucial to libertarians, let's proceed to *how* to make the judiciary more transparent.

Sometimes, the rulings or orders of court cases have been uploaded to the Internet; it just becomes a matter of finding them. For example, the United States Supreme Court uploads the [latest slip opinions](#) and [volumes 502 – 561](#) to their own website; otherwise, you'd need to check older cases on websites such as [OpenJurist](#) or the [Legal Information Institute](#) at the Cornell Law School. Unfortunately, it is rather common for district or appellate federal courts to have their case documents behind a [paywall](#) (usually [PACER](#)), unless the corporate media releases them for a story; thankfully, [hacktivists](#) such as [Carl Malamud](#) and [the late Aaron Schwartz](#) proved it was possible to emancipate federal court documents from behind the PACER paywall into the public domain.

Oddly enough (or perhaps not?), the Texas judiciary does not have as much of a paywall than the federal judiciary, considering the [TAMES case search](#). For instance, you can use TAMES to locate all the court documents for a particular case in easily downloadable PDF format – here are all the documents for the infamous 2014 [Zahher El-Ali v. State of Texas](#) case involving [civil asset forfeiture](#) (spoiler! Mr. El-Ali will never get his pickup truck back, and the rest of us Texans have no property rights whatsoever – [Judge Willett said so!](#)). During two of my [political fieldtrips](#) last year, I discovered that the county and municipal governments each have what they call “[records inquiry](#),” or “[public inquiry system](#),” however, keep in mind that these [court dockets](#) are simply the court schedules and not the case documents themselves.

Once you've got the documents, it's time to organize them in preparation for sharing them publicly. Most likely, you will have to re-label the PDF files into a format that works for you. What Shane has done with the [political prisoners archive](#) is to use the following format:

DATE – DOCUMENT TYPE (NAME OF CASE).PDF

The date is shown with the last two numbers for the year, then the month, followed by the day of the month; this is done so that when visitors to *Liberty Under Attack* download court documents, they are automatically arranged chronologically in whatever folder they decide to put them in. For example, a document appears as such:

[150417 – Indictment \(United States v. William Wolf\).pdf](#)

“150417” means April 17th of 2015. You also know that this is the indictment for William Wolf's case; obviously, “United States” could be shorted to “U.S.” but that is more of an aesthetic preference than anything else. Most importantly, you want to make sure that there is a hyperlink associated with a particular court document, so what this means is that you will have to upload the PDF file onto your own website, blog, or file-sharing account.

Whatever you do, do not use [Scribd](#), because any documents uploaded to that horrible website require you to login first before you are able to download anything, which might as well be a paywall – the idea here is to make these court documents easily downloadable for the most casual Internet surfer.

As soon as the court document files are hosted and available for free download by anyone, then you need to promote those hyperlinks. One easy way of doing so is to record a short screencast [vlog](#) of you reading some of the document, uploading the video onto a video-sharing website, and then adding the hyperlink to the video description box; if the document's hyperlink is too long, then you will need to first make a [shortlink](#), and then put that shortlink in the video description box. Another way is to put together a webpage for a specific political prisoner and hyperlink all the documents for his case on that one page, add a picture of the prisoner so as to humanize him, create a shortlink for the entire page, and then record a vlog advertising for the entire page. Yet another way is to call-in to live-streaming podcasts and wind the conversation over to your political prisoner whom you want to promote, and then mention the shortlink for the entire page so that the listeners know where to go to see and get the court documents for themselves. You can also promote your assemblage of court documents through discussion forums, email lists, and even Fascistbook!

If any of the alleged “supporters” for these political prisoners truly cared about them, they would be pushing for judicial transparency instead of frittering away donations for [legal defense fund scams](#), or [signing fruitless petitions](#). Although there is nothing wrong with making [FOIA requests](#), that is not usually the first move to make, unless the nature of the case forces you to deal with “national security” issues. Admittedly, [Ian Bernard](#) does a very good job uploading both court documents and trial footage onto [Free Keene](#) and its accompanying [YouTube channel](#), but everything is scattered across multiple blog posts, and is not organized on an easy to locate webpage or playlist, such as the [Free Keene Video Archival Court Footage, 2008 – 2014](#).

Ultimately, the truth of the matter is that the Internet allows common people to make government court documents publicly available nearly for free, or otherwise, at cost. The learning curve will be fairly short for you if you take this tutorial presented here seriously. If you are concerned about your individual privacy, then be sure to either learn how to use proxy servers in order to obfuscate your internet protocol (IP) address being traced back, or use a public WiFi spot, or use a “clean” computer from which to upload, or some combination of the aforementioned methods, but regardless, don't let your fear of being discovered get in the way of you getting those documents up!

Conclusion

When it comes to the importance of judicial transparency, it can be summed up thusly: if the Denver Broncos have never looked at the playbook, they're going to have a hard time winning football games. Just as with the cheesy metaphor, if “we” don't know what the government is arguing in their own courtrooms, it's going to be hard to try and get “our guys out of prison.” To

provide another example, it's much like a blind man entering a boxing ring—if he can't see his opponent, then he can't see the punches that he would need to dodge, at the very least.

The goal of judicial transparency, is to make public [open-source intelligence](#) about the government judiciary, so that American dissidents can make their own decisions, when it comes to avoiding incarceration, especially when considering the exorbitant amount of “victimless crime” laws. It is our hope that the alternative media will begin utilizing the system that we have explained previously, and adapting it for their own purposes, as they see fit.

For more great content like this, please consider [donating](#) to *Liberty Under Attack*. Alternatively, sign up for a [free trial](#) through Audible, receive a free audiobook, and help support us in the process. Lastly, make sure to sign up for [LUA email updates](#).

Secured Record Archival: How to Protect Your Documents from the Government

www.thelastbastille.com/2016/07/01/secured-record-archival-protect-documents-government/

“Do you know where your chief of police lives? Do you know his telephone number? What sort of car he drives? How much money he’s got in the bank? Do you know what insurance company insures his life or his home and so on? I bet you don’t know any of that information but you can rest assured that your chief of police has access to all of that information about you.”

– The Anti-Terrorist



Introduction

Trusting faceless third-parties to keep your records private is downright foolhardy, especially considering just how ridiculously easy it is for adversaries to gain access and deprive you of them. Almost two years ago in 2014, [nude celebrity photographs that were originally stored on Apple’s iCloud were leaked](#); about a year ago in 2015, [the Ashley Madison data breach occurred](#). What these episodes teach us is that anyone’s private records are potentially susceptible to being made public against their will.

Some individuals, particularly those of older generations, seem to have the tendency to place too much faith in [legal interstices](#) in order to protect their records. Although certainly well-intentioned, the fact of the matter is that relying on [originalist interpretations](#) of [constitutional law](#) is fraught with perilous trapdoors laid by the [insufferable bar attorneys](#). Simply put, the government uses [color of law](#) as a key feature of its [lawfare](#) strategy against Americans.

[Defensive computing](#) holds better promise for securing your records than any legal remedies. Undertaking the

responsibility upon yourself alone for securing your archived records quickly becomes much more of a pragmatic question, which appears to be one that quite a number of people would rather just avoid. Whether it be due to computer illiteracy or moral cowardice, technological innovations for both digital and paper records are routinely ignored by not only [disingenuous activists](#), but also by their incompetent followers alike.

An overview tutorial for how to securely archive both your digital and paper records will also be included within this article. References to more detailed information will be mentioned and listed, as well as specific recommendations for Macintosh users; behavioral guidelines will be littered throughout, yet, they can be easily adapted to suit computer users of any operating system. Good habits for sorting paper records are outlined and the question of [digitization](#) will be broached.

What must not be forgotten, however, are the implications for secured record archival within the broader scope of [security culture](#). Much like [home hardening](#), secured record archival depends upon layered security not unlike an onion, especially when it comes to multiple backups of the exact same information spread out onto different storage mediums. [Security audits](#) are the only real way to tell whether a tool or practice is objectively effective or not.

PART I

Constitutionality & Case Law of Fourth Amendment “Papers”

During my recent examination about [whether cellular telephones increased human liberty](#), the legal question of what counts as “papers” under the Fourth Amendment of the [United States Constitution](#) was posed, but not answered. The [Fourth Amendment](#) says:

*“The right of the people **to be secure** in their persons, houses, **papers**, and effects, against unreasonable searches and seizures, **shall not be violated**, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and **particularly describing** the place to be searched, and the persons or things to be seized.” [emphasis added]*

Obviously, it does not take an adherent of [original intent](#) legal theory to deduce that the American people are to be secure in their papers **except** when issued search warrants **particularly describing** the location being searched and the individuals and property being seized. This is the **only** exception to the rule of the people enjoying secured papers; otherwise, this legally acknowledged right of the people to be secure in their papers **is being violated**, which is **specifically prohibited** by this constitutional amendment.

[The Anti-Federalists](#) warned the American people against [ratification of the federal Constitution](#), because they easily foresaw how the central (general) government would try to run roughshod over the member state governments within the Union. Brutus told New Yorkers that the [Supremacy Clause](#) (Art. IV cl. 2) renders the several state constitutions pretty moot, if not also null and void, hence the necessity for a *federal* bill of rights [[Anti-Federalist #84](#)]. His concern was that absent something like the Fourth Amendment, [writs of assistance](#) (aka, general

warrants) would reemerge as the incorrigible scourge that they were as enforced by the Redcoats, but this time, by the federal government.

Just so that there is no misunderstanding about this constitutional exception of the people being secure in their own papers, let's briefly peruse what exactly the words, "particular" and "describe" meant to the Framers within the context of the Fourth Amendment. According to Webster's 1828 Dictionary, "[particular](#)" meant "pertaining to a **single** person or thing; *not* general" – by the same token, "[describe](#)" means "to show or represent to others in words; to communicate the resemblance of a thing, by naming its nature, form or properties." Combining the words "particular" and "describe" into "particularly describing" would seem to mean that search warrants must be specifically detailed in the location they are searching and the individuals and property they are seizing; absent this rather narrow scope, the rule of people's records being secure is clearly enumerated.

Unfortunately, today's search warrants are so overbroad that they might as well be writs of assistance. Much like [the despicable history of Social Security](#), the rule of the Fourth Amendment's prohibition against warrantless searches and seizures has become narrower than the exceptions to it. Simultaneously, the scope of *warrantless* searches has bloated to the degree that it is increasingly difficult to successfully litigate against a police officer's conduct across a variety of circumstances when he executes a warrantless search.

Probably the most dangerous exception to the Fourth Amendment's [Warrant Clause](#), within the context of being secure in one's papers, is known as **searches incident to a lawful arrest**. Also known as the [Chimel rule](#), this exception holds an arrested suspect is subject to a warrantless search of not only his person, but also whatever property he has within arms reach; anything that may be construed by the officer to be evidence of a crime as a result of this warrantless search cannot be later suppressed as evidence upon request of a [motion](#) in court. Other exceptions to the Warrant Clause include consent, plain view, "exigent circumstances" (like a [Terry stop](#)), foreign intelligence surveillance (think [dragnet wiretapping](#)), automobiles, international borders, public school grounds, and prison cells.

Given that the exceptions are broader than the rule, it is not totally crazy to think that the rule seldom matters (in much the same way that Social Security is voluntary, legally speaking, yet because the exceptions to this rule involve [tax liabilities](#), [automobile registration](#), [driver licensure](#), and [welfare handouts](#), Social Security is, for all practical purposes, **coercive**). The [exclusionary rule](#) is the foundation behind motions to suppress evidence, and it is the basis for enforcing the Fourth Amendment's prohibition against general warrants; unfortunately, the applicability of the [fruit of the poisonous tree](#) doctrine has shrunk while the exceptions to the Warrant Clause have grown. What this means is that the exclusionary rule now possesses glaring impotency in direct proportion to the color of law being practiced by the government; the fact that judicial case precedent now has grades of legal interstices between homes (greatest legal protection), cars (medium legal protection), and your physical person (least legal protection) is patently ridiculous, because all three of those are covered **equally** by the "persons, houses, papers, and effects" within the wording of the Fourth Amendment.

Having given you the lay of the land, let's now peruse specific examples, beginning with warrantless searches. *Terry v. Ohio*, [392 U.S. 1](#) (1968) ruled that police may **briefly** detain a suspect without arrest. *Chimel v. California*, [395 U.S. 752](#) (1969), ruled that an **arrested** suspect's person may be searched without a warrant, and that anything found on him may be used against him later in court by the prosecution; however, anything exceeding arms reach of the arrested suspect requires a search warrant. *United States v. Robinson*, [414 U.S. 218](#) (1973) ruled that contraband found on an arrested suspect as a result of a search incident to lawful arrest (according to the *Chimel* rule) cannot be suppressed evidence via the exclusionary rule. *United States v. Rodriguez*, [995 F.2d 776](#) (1993) ruled that an address book found on an arrested suspect as a result of the *Chimel* rule cannot be suppressed evidence, either; interestingly enough, *Rodriguez* was used alongside *Robinson* to deny an appeal for a conviction secured in *United States v. Abel Flores-Lopez*, [No. 10-3803](#) (2012), the circumstances of which involved the warrantless search of a cell phone.

Since the federal case law involving warrantless searches has established a precedent for increasingly broad

exceptions based upon the most nuanced of minutiae, then would it be safe to assume that the case law involving search warrants obey the limitations imposed by the Fourth Amendment? Generally speaking, if police officers consider your records to be either [contraband](#), [evidence of a crime](#), or [an instrumentality of a crime](#), then they will seize it. Three cases bear closer scrutiny, for the language within these search warrants is an affront to both the letter and the spirit of the Fourth Amendment.

On June 4th of 2014, Robert Beecher was indicted for being a **felon in possession of firearm**, in violation of [18 USC § 922\(g\)](#). According to “Amendment B” to [the search and seizure warrant of May 6th](#), it said:

1. Records and documents which reflect the sale, trade, pawn, receipt, or disposition of any firearm, ammunition, and/or firearm components and accessories, buyer lists, seller lists, books reflecting the value of firearms or ammunition, and notes (cryptic or otherwise), pay-owe sheets, records of sales, log books, ledgers, documents, shipping records and indicia, materials used to package firearms and ammunition for shipment, and photographs which reflect relationships between unidentified co-conspirators to include personal telephone/address books, electronic organizers, and rolodexes.
1. Records that establish the person who have control, possession, custody, or dominion over the property and vehicles searched and from which evidence is seized, such as: personal mail, checkbooks, personal identification, notes, other correspondence, utility bills, rent receipts, payment receipts, financial documents, keys, photographs (developed or undeveloped), leases, mortgage bills, vehicle registration information or ownership warranties, receipts for vehicle parts or repairs, telephone answering machine introductions, and fingerprints.
1. Documents and manuals that depict or instruct on subjects such as firearms conversion kits or parts, automatic weapons concealment, smuggling, or state and federal firearm and ammunition laws.
1. Safes, strong boxes, and/or other secure receptacles for the maintenance of valuable items, firearms and/or documents including books, records, and any keys or other evidence of the existence and use of any lockers, safety deposit boxes or other secure receptacles located elsewhere than at the premises.
1. Computers, to include all electronic data stored in the computer such as photos, documents, notes, correspondence, firearms records, financial records, names, addresses, telephone numbers, and other records relating to the acquisition, purchase, transfer, possession, manufacturing and/or disposition of firearms.
1. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items:
 - a) Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;
 - b) Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
 - c) Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMS, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
 - d) Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;
 - e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

- f) Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and
- g) Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data. [emphasis added]

Not only was the language overbroad, but when a search warrant uses all-encompassing adjectives to describe common nouns, then I think it is more than fair to say that the *specificity requirement* (“particularly describing”) of the Fourth Amendment is not being obeyed here. Ultimately, Beecher took a [plea agreement on April 2nd of 2015](#) in order to spare his daughter Jessica from being prosecuted herself; he is expected to be released sometime in 2025.

Schuyler Barbeau was [originally indicted on December 16th of 2015](#) for **possession of unregistered firearm** in violation of [26 USC §§ 5861\(d\) & 5845\(a\)\(3\)](#); on February 25th of 2016, a [superseding indictment](#) tacked on the additional charge of **possession of a machine gun** in violation of [18 USC §§ 922\(o\) & 924\(a\)\(2\)](#). According to “Amendment B” to the [search and seizure warrant of December 5th](#), it said:

All documents and items reflecting evidence and/or fruits of the commission of the crimes of (a) unlawful possession of a firearm, in violation of Title 26, United States Code Sections 5861(d) and 5845(a)(3); (b) possession of stolen federal property, in violation of Title 18, United States Code, Section 641; and (c) possession of a machine gun, in violation of Title 18, United States Code, Section 922(o), including:

- Any documents, including books, pertaining to any explosives or short-barreled rifles;
- Transaction Records: Documents such as ledgers, receipts, notes and similar items relating to the acquisition of any explosives or short-barreled rifles.
- All documents reflecting the ownership or possession of any explosives or short-barreled rifles.
- Documents sufficient to show dominion and control of the premises and areas searched.

Similar to Beecher, Barbeau’s search warrant was a grab bag scarcely itemizing what the government police were “authorized” to search and seize. Barbeau is currently incarcerated because his case is still being adjudicated; his next court appearance is scheduled for November 7th.

Back in 2008, the home of John and Jacqueline Stowers was raided by “local” government police for failure to hold a license required for retail food establishments, pursuant to [Ohio Revised Code § 3717.21](#). According to the [search warrant of November 26th](#), it said:

*“The search is made for certain evidence, to wit...invoices, orders, bills of sale, applications and customer lists or other business **records** tending to show the conduct of a retail business including personal property and **documents** tending to establish the identity of the person/persons in control of the premises as well as customers, employees, owners, agents, sales persons, and assigns of the business...**any and all documents** representing proceeds from the commission of criminal offenses; and **bank records, any ledgers**, and safes, any information regarding safety deposit boxes, and safety deposit box keys or entrance/access media; **any investment accounts records; any computers, any external electronic storage media**, including, but not limited to floppy discs, DVD’s, CD’s; **any external data drives**, including, but not limited to, thumb or flash drives; **any and [all] cell phones**, pagers, Blackberrys, Sidekicks, PDA’s and **any accompanying records** for such devices; **any documents** establishing an ownership and possessory interest in any real property and any contraband...”* [emphasis added]

Although the federal government was not involved in prosecuting the Stowers, the fact of the matter is that due to both the [Tenth Amendment](#) and the jurisdiction of the acting government, the [Ohio Constitution](#) is controlling. Art. I § 14 of that constitution says:

*“The right of the people **to be secure** in their persons, houses, **papers**, and possessions, against unreasonable searches and seizures **shall not be violated**; and no warrant shall issue, but upon probable cause, supported by oath or affirmation, **particularly describing** the place to be searched, and the person and things to be seized.” [emphasis added]*

Much like the Fourth Amendment, the specificity requirement is operating within Art. I § 14 as the only constitutional exception to otherwise being secure in one’s papers. This language of “any” and “all,” when used to describe ledgers, records, documents, manuals, and even computers, violates constitutional particularity. Appellate judge Eve Belfance wrote the following [Decision and Journal Entry on June 6th of 2011](#) regarding the Stowers’ case:

“The trial court entered a judgment order that property seized in the execution of the search warrant be returned to Appellants and later granted summary judgment to ODA [Ohio Department of Agriculture] and LCGHD [Lorain County General Health District] on other claims. Appellants appealed and this Court issued an order remanding the case to the trial court for the limited purpose of disposing of the search and seizure claims, which the parties had intended to voluntarily dismiss. Those claims have now been dismissed and Appellants appeal the trial court’s order granting summary judgment against them on their remaining claims for declaratory judgment, injunction against enforcement, and attorney fees. Appellants present two assignments of error.”

This is rather intriguing, for it means that the Stowers managed to get their property back, but they pursued the Ohioan government in the attempt to discover the legality behind the raid itself. Judge Belfance concludes:

“Appellants’ first assignment of error is overruled because Appellants operate a food retail establishment subject to Ohio’s food safety laws, including R.C. 3717.21. Appellants’ second assignment of error is overruled because Ohio’s food safety laws are not unconstitutional as applied to Appellants. Accordingly, we affirm the judgment of the trial court.”

Apparently, a **private membership organic food-buying co-op** is considered by the Ohio judiciary to be a “retail food establishment” subject to licensure, just because they said so; as such, this is the Ohio government’s primary

justification for [the police raid on Manna Storehouse](#). I seriously doubt Chad Stowers, one of John and Jacqueline's adult children, reenlisted in the U.S. Navy for another tour in Iraq once he heard of what happened to his parents and siblings, don't you think?

What is to be learned from these case precedents in both warrantless searches and search warrants? I think it means is that proposed "reforms," like requiring greater specificity in terms of distinguishing between **physical** searches and **digital** searches within search warrants *does not* solve the problem of "searches incident to lawful arrest" or the blanket general warrants' overbroad language of "any and all documents." [Orin Kerr's 2005 white paper](#) lays out nothing less than a false solution to the problem of systematic constitutional violations against the Fourth Amendment; besides, distinguishing between physical and digital searches completely ignores the **seizure** involved of the computers themselves. As far as I am concerned, Kerr is either totally incompetent or intellectually dishonest, and the fact that the Mississippi Law Journal published his paper really makes me question just how rigorous their [scholarly peer-review](#) actually is in reality.

Absent a technological solution, is there anything that can be done to thwart the government's exercise of lawfare against the security of your papers? Much like how drug dealers would flush their illicit narcotics down the toilet, I think the idea of a "purification" ritual before an **expected** arrest would be wise. If you pretend that you are "purifying" yourself before "the Lord, your government," chances are that your subsequent [police interrogation](#) will be a lot easier to navigate. Should you stash your records in a hidden place **before** the police give you the "once over" as part of a *Terry* stop and/or in accordance with the *Chimel* rule, then with any luck, you might just win by keeping your freedom and maybe even your papers too!

END PART I

PART II

Digital & Paper File Hardening

Secured record archival, briefly defined, is the disciplined practice of organizing, locking, and hiding both your digital and paper records. This is done with the explicit purpose of hardening an individual's life by preventing it from being susceptible to compromise; in other words, to lessen any [vulnerability to coercion](#). Any successful implementation of such a targeted strategy relies not only upon the efficacy of the methods themselves, but also the harmonious utilization of them together.

Before any records can be secured, they must first be archived. Archiving one's records presumes that they are organized in a clear and consistent manner. Lacking this, such disorganized records need to be sorted, prioritized, and erased as appropriate.

Sorting files is one of my least favorite things on this planet to do. It is a rather tedious process of examining and judging the fates of each individual record I currently have in my possession. As time passes, some records maintain their importance, whereas others become quite irrelevant; most are irritatingly somewhere in between.

You should consider taking [a rather "minimalist" approach to sorting your paperwork](#). What [you learn from sorting your paper records](#) can transfer over to doing so with your digital ones without too much of a fuss over adaptation. Although [how to organize your paper records can be individuated](#), I think the core idea here is to reassess your

priorities, and by doing so, you can [more easily strip away all that excess baggage](#) that fails to bring value into your life. [Emotionally letting go of sentimentality](#), whether that be taking the Giant Leap or through Baby Steps, is integral towards getting your paper records under control by reducing your overall level of clutter.

Organizing digital records is, in many ways, awfully similar to sifting through your paper records. Categorizing can be done according to subject matter, [filename extension](#), or some combination of the two; manageable [file folder](#) sizes are the goal here for ease of archival. Please do keep in mind, though, that secure deletion (aka, “wiping”) of [computer files](#) is just as important as shredding, for both are demonstrable ways of [lightening the load](#). Digitization has truly shown [the possibility of paperless](#) recordkeeping, if in no other way than for reducing stacks of unsightly paperwork.

Sorted files ought to be inventoried, so that you can have a quick reference guide as to where everything is located. For example, knowing where [your will, living will, and emergency contact information](#) is located will certainly make life much easier for your loved ones should you ever become incapacitated. These inventory lists will also minimize unintentional redundancy of the same files being endlessly copied and recopied, which do seldom else than take up valuable megabytes and gigabytes.

Archival is mainly a process of storing your organized files onto multiple storage devices. Storage mediums range from burnable CDs and DVDs to flash drives and external hard drives. Ideally, you should also perform a full backup of your entire hard drive, but if this is not possible, then you ought to conduct an incremental backup, beginning with your current working documents, email address book, [encryption keys](#), and password manager.

Once your records have been organized and archived, then you must secure them; this is accomplished through locking paper records and encrypting the digital ones. After you have placed your paper records inside [punched pockets](#) within a [filing cabinet](#), you can [install a locking bar](#) that is then secured with a padlock, but be forewarned – much like how [luggage locks can be defeated using a ballpoint pen](#), a [multi-wheeled combination lock can be bypassed with nothing more than a thin sheet of metal](#) (even those [three-wheeled locking attaché briefcases](#) can be cracked!). Maybe if a padlock on your file cabinet’s locking bar required a unique key instead of a combination to unlock, then that key could be hidden in a different location away from the prying eyes of criminals and other miscreants, or perhaps noiselessly if it were stored on a [compact key holder](#) inside of, or next to, something else that is otherwise in plain view.

[Computational security](#) is directly proportional to [key size](#), so the longer they are, the better security you enjoy. This is why the term “password,” has been supplanted by *passphrase*, because the whole idea behind good computational security is longer key size, and “password” implies a shorter one than does passphrase. [According to Arnold Reinhold](#), longer all-letter passphrases have higher bits of entropy than does a shorter password that intermixes some English upper and lowercase letters with punctuations, numbers, and symbols. [Joseph Bonneau found that multi-word passphrases are not randomly chosen enough](#), yet, Reinhold’s [Diceware method](#) is the only real solution to that problem of lower entropy passphrases that I’ve been able to discover.

Encryption is grossly overblown yet seldom understood. Full-disk encryption used to be all the rage, at least until [David Hulton demonstrated his vfcrack cryptanalytic program back in 2006](#), which completely exposed the security holes in Apple’s FileVault utility. [A 2008 research project](#) discovered that cold boot attacks were successfully mounted against popularly known full disk encryption systems; not only that, but these researchers discovered that FileVault kept multiple copies of the user’s login password in memory, which are vulnerable to imaging attacks. Ultimately, Dr. Eric Cole postulated that [full disk encryption gives a false sense of security](#); he recommended using file encryption, instead.

[User error](#) is a fear that, while justifiable in particular circumstances, is frequently exaggerated due to other mitigating factors, such as software infections or hardware breakdowns. The main reason people don’t use encryption or locks is that they are primarily concerned *not* with having their information being stolen or otherwise used against them, but rather, having their access to such information being blocked, mainly due to forgetting their

passwords or misplacing their keys. Two methods that could be used to overcome these fears is to use a [password manager](#) program (software application) and a [laptop lock](#) whose key is kept on a [compact key holder](#) (hardware solution).

Records that have been archived and encrypted are not yet fully secured until they have been adequately hidden from casual observation. Caching archived documents typically involves moisture protection for both paper and digital records. [Disposable diapers](#), [Teflon tape](#), and [desiccant sachets](#) (or in a pinch, [uncooked white rice](#)) can be all pressed into service as moisture absorbers, as appropriate to the cache space itself.

Truly the best defense against cryptanalytic devices like [Cellebrite's UFED](#), which can reportedly **bypass user locks and decrypt data**, is to prevent your archived records from being discovered by both burglars and the [Bluecoats](#) in the first place. Absent this, the next best thing to do is to use [free and open-source software](#) and [open-source hardware](#) to create as many security layers as possible, even if only for the purpose of delaying the inevitable. Generally speaking, I recommend that you peruse these defensive computing guides for more detailed information on how to do this:

- Electronic Frontier Foundation's [Surveillance Self-Defense](#) project
- Tactical Technology Collective's [Security in-a-Box](#) project
- Thomas Reeds' [The Safe Mac](#) computer security blog (Mac OSX only)
- Peng Zhong's [PRISM-Break](#) open-source computer security program directory

[Claire Wolfe recommended](#) assembling a document file of online usernames and passwords, encrypting it, and then wiping the original from your hard drive; at least two copies of the **encrypted** file are to be hand delivered to trusted contacts for safekeeping. She also advised that the same thing be done in a separate file containing credit card and bank account numbers. Finally, Wolfe suggested learning how to configure password locking on your laptop and to use full disk encryption; regarding the latter item, I side with Dr. Cole instead by favoring file encryption myself.

A Layman's Tutorial on Performing Secured Record Archival

Now that you understand both the legalities and technologies undergirding secured record archival, it's time to show **one** way how defensive computing could be used synergistically to provide the best security possible for your archived records. The following tutorial will demonstrate how to utilize a variety of computer programs and other methods in order to provide comprehensive security layers. Any other combination of software and operating systems are not necessarily applicable for this example tutorial.

There are five sequential phases to this tutorial. Each one of them uses different techniques, some that are physical, others that are digital, and a few that are both. They are:

1. Scan
2. Inventory
3. Backup
4. Encrypt
5. Cache

Scan involves not just antivirus and anti-malware programs, but also the digitization of paper records. **Inventory** determines just how much and what kind of records there actually are, with the goal of being able to reduce the extraneous clutter, whether in your filing cabinet or on your hard drive. **Backup** spreads out all the organized records amongst dissimilar storage media, so that in the event one of them fails or is otherwise inaccessible, your

data can still be accessed via an identical copy. **Encrypt** is a layer of actual security, although this is mostly applicable to digital records only. **Cache** is the other layer of security that applies equally to both digital and paper records through the use of physical hideaways.

On a [MacBook](#) running [Mac OS X Snow Leopard](#), an antivirus scan can be done by [Avast](#), an anti-malware scan by [ClamXav](#), and an anti-keylogger scan by [DetectX](#). The health and well-being of your hard drive can be determined by the “verify disk permissions” and “verify disk” buttons within [Disk Utility](#) (if needed, the repair buttons for both are in the same window, but please keep in mind that when I had to repair my hard disk a year and a half ago, I had to boot up my laptop [from the operating system installation CD itself](#), and then run Disk Utility’s disk repair from there). Any sort of [digitization](#) involving [image scanning](#) of physical documents into PDF files is usually accomplished via [Preview](#).

An inventory of your hard drive’s archival status can be done by accessing the metadata of both files and folders by right-clicking them and then selecting the “Get Info” field within the [Finder](#)’s drop-down menu; these inventories can be documented by arranging the metadata windows and then taking cropped screenshots, which are subsequently labeled thusly:

141129 – hard drive archival status.jpg

Just as with [openly-sourced archived court documents](#), “141129” in this example means November 29th of 2014. In a somewhat different vein, a **cumulative flash drive archival inventory** can be listed via a [Microsoft Word](#) .doc file or [Microsoft Excel](#) spreadsheet, and then the most current copy of which can be rendered into a PDF file for archival purposes. Also, all USB storage media should be scanned using programs like Avast and ClamXav *before* they are loaded down with archived records.

Speaking of thumb drives, once you have finished the insipidly odious drudgery of sorting and organizing your digital records, then Disk Utility’s erasure of free disk space ought to be performed on the hard disk as well as any other storage media you can plug in, like [USB flash drives](#) and [external hard drives](#) (please note that newer Mac operating systems like [El Capitan](#) have “grayed out” the ability for Disk Utility to [erase free disk space](#) and even [secure deletion](#)). [CD-Rs](#) and [recordable DVDs](#) can have computer files “burned” onto them, but do keep in mind that unless you are using [CD-RWs](#) or rewritable DVDs, these [optical disks](#) are one-trick ponies, so it would behoove you to also make a **cumulative CD/DVD archival inventory**, as well.

Before using any form of encryption, you must invent passphrases you can memorize, or at bear minimum, those that you are comfortable enough [writing on a piece of paper](#), which, in partial contrast to Bruce Schneier’s recommendation, is itself located somewhere innocuously. Probably the most secure form of password generation is the [Diceware technique](#), which uses five [dice](#) and the [Diceware master word list](#). Arguably, the best way to keep track of all your passphrases, aside from [rote memorization](#), is using a [password manager](#) program like [KeePassX](#). When it comes to file encryption, you could use Disk Utility to create an [encrypted disk image](#); alternatively, if you’ve installed [GPGTools](#) as part of [configuring PGP for email encryption on a Mac OSX](#), then you could just simply right-click on any file or folder, highlight “Services,” and choose the “OpenPGP: Encrypt File” option. If you’re the *really* cautious type, then you may want to consider incorporating the [dual layer encryption method](#), which blends low-tech with high-tech cryptography.

Whether a cache take the form of a physical hideaway or [cloud computing](#), there is much to be learned about this particular skill set. The following trilogy of books can help get you up to speed on the basics of squirreling away your records discretely:

- Michael Conner’s [How to Hide Anything](#)
- Jack Luger’s [The Big Book of Secret Hiding Places](#)
- Dennis Fiery’s [How to Hide Things in Public Places](#)

Obviously, practice in an environment with the lowest possible risk to yourself should you become discovered, and be sure to have a plausible [legend](#) rehearsed ahead of time. For example, should you decide to stash your “[little black book](#)” inside of a [zipper storage bag](#) somewhere, then make sure that all of your high-priority information is encrypted on at least *two* different storage mediums, one of which is located at home, and another stashed away from home.

END PART II

Conclusion: Observations on Strategic Implications

Lawfare is an existential threat, yet, there has not been any [risk analysis](#) I know of that has been performed in order to gauge the likelihood of its occurrence to individual American citizens; that being said, never underestimate the [Al Capone method](#) that has been used by the government police time and time again. Upon examination of the legal interstices concerning seizures and search warrants, it would seem to be the case that the exclusionary rule’s applicability in enforcing the Fourth Amendment through motions to suppress evidence has become noticeably impotent. Although there may be some exploitable loopholes circumstantially from time to time, gambling your property and liberty on the odds that you will be able to regain the former and retain the latter through any form of [legal procedure](#) seems rather naïve to me.

Some might argue that [Moore’s law](#) is what is truly driving the ongoing [crypto wars](#), but even if true, I don’t think that it’s solely responsible, for the allure of absolute power should never be underestimated. Apparently, it would seem to be the case that the [wannabe omniscient NSA](#) has a “[Tailored Access Operations division](#)” that is literally composed of [black hats](#). When you consider the invasiveness of cryptanalytic devices like the UFED, or the inability of newer Mac OSX users to natively secure delete or otherwise erase free disk space, it really does beg the question of whether crypto-anarchists are truly even worth a damn anymore.

What has been seldom touched upon in any of the modern cryptographic literature is the nuts and bolts efficacy of most encryption programs on both sides of the crypto wars. Regardless of whether they be proprietary or open-source, almost no one has conducted and released [security audits](#) for these programs. Exceptions to this include:

- Tom Berson’s 2005 [Skype Security Evaluation](#)
- Thomas Reeds’ 2012 – 2014 [antivirus & malware scan tests](#)
- Omar Choudary, et. al.’s 2012 [security analysis of FileVault on Mac OSX Lion](#)
- Taylor Hornby’s 2014 [10-hour security audit](#) of [EncFS](#)
- NCC Group’s 2015 [cryptographic review](#) of [TrueCrypt](#)

Perhaps crowdfunding might incentivize some programmers to examine the source code for any of the programs listed on Peng Zhong’s [PRISM-Break](#) directory, but quite frankly, what value is the right to privacy in a civil society if none of the free software advocates are willing to conduct and publish security audits for the very programs they wholeheartedly recommend the common man to pick up and use, or shall I say, download and install? Personally, I think the closer that defensive computing emulates something like the [Dark Android Project](#), the better off the hapless citizenry will be; how does the concept of a Dark Mac, a Dark Windows, or a Dark Linux sound to you?

Passively assuming that digital encryption programs have a viable efficacy based solely on faith alone is not good enough anymore – **Americans need proof that they work**. For my own initial wishlist, I’d like to know what security

audits would potentially reveal about [KeePassX](#), [GPGTools](#), and [Safe](#). Although I understand that [security audits can be quite costly](#), as was the case with SpiderOak's [Crypton project](#), yet, if [over 116,000 people donated \\$6,675,039 in 17 days](#) because of the recent [Orlando nightclub shooting](#), then why can't a cheaper bill be footed so that fewer individuals find themselves becoming [political prisoners](#) on the mere accusation of having committed a [victimless crime](#)?

Similar to [home hardening](#) and [dual encryption](#), secured record archival incorporates multiple layers of security, much like an onion. This layered security approach can be used in a digital context by using a [Kensington security slot](#) simultaneous with a password lock and file encryption, as well as in a more traditional paper one via a keyed padlock on the locking bar for a file cabinet that also happens to possess a [false bottom](#) inside it. Deliberate redundancy in multiple containers is quite wise, for it would be rather foolish to place all of your most important eggs in one basket.

At the end of the day, secured record archival makes you "[vonuer](#)," that is, comparatively more invulnerable to coercion. Even though secured record archival might provoke feelings of anxiety in some individuals, this should be taken as a sign that you are feeling quite vulnerable, so the best **action** you can take is to *strategize* how you can begin lessening that vulnerability as best as you can with what you currently possess and are able to afford. If for no other reason, this is why secured record archival gives you piece of mind once you have overcome the initial hurdle of learning the lingo, the concepts presented, and how to custom tailor it to your own lifestyle.

Keeping Your Own Counsel

▫ www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/

1/1/16 UPDATE: In learning more about [security culture](#), I realized this article really needed a serious overhaul. Entire paragraphs have been deleted, and brand new ones added; sentences have been noticeably edited, and a few elements have been kept from the original version. I sincerely hope this revision is more helpful to you all.

Full spectrum dominance is all based upon the complete predictability of a targeted population. A surveillance society is only possible if the captive public throws caution to the wind by divulging every inane thought that comes into their heads. Reverence for privacy must be reinvigorated if any of us are going to have a meager chance at exercising any of our common freedoms.

Privacy is all about the control of information.

Whatever you choose to discuss reveals something about yourself. Contrary to popular belief, you retain absolute control over what comes out of your mouth, even if you are being coerced. Written text and verbal speech are evidence that you are in charge of your own faculties, for it requires a minimum of self-control in order to express yourself.



American dissidents who commit themselves to transparency should really heed the warning that [not all truths need to be said](#); pointing out the injustices of [the State](#) is one thing, but airing your neighbor's dirty laundry is completely different.

While it may be possible to hook an audience with salacious tabloid nonsense, in order to reveal true atrocities, it is counterproductive. Being misunderstood, ineptly judged, or cowardly decried is too great a risk. Given that time is finite, why gamble on derailing any positive outcomes with reckless gossip?

Some of you may be familiar with the concept known as [operational security](#) (OPSEC), which has been popularized by survivalists like [James Wesley, Rawles](#). Although it is commonly understood that OPSEC entails the use of various privacy measures, I must ask as to what is the nature of the active operation in question? Perhaps [information security](#) (INFOSEC) is a more accurate acronym?

What information, though, would "count" as being within the bounds of INFOSEC? Consider what details would be valuable to the government police during one of their investigations. I would suggest that, for instance, [personally identifiable information](#) (such as your [Social Security number](#), or the legal names of your [security team](#) members), the passwords for your encrypted data, and the location of your supply caches, are but just some of what ought to be considered as INFOSEC. Indiscriminately spouting this knowledge over [the Internet](#), or revealing it during a [police interrogation](#), could result in harm to yourself or others.

When someone tells you something in confidence, you are expected to keep it private. Surreptitiously recording VoIP calls has come up more than once – I have been asked if I would mind being recorded on a private conference call, which I responded to by saying that I did; on another occasion, a third-party asked, of whom I was talking to, if a previous conference call between the three of us had been surreptitiously

recorded, to which he responded that it had not been (thankfully). Intimate or sensitive details can be used to sabotage relationships, so those who betray confidences ought to be [blacklisted](#) as untrustworthy gossips.

Regarding your own personal identity, limiting what you say about yourself to others can help keep you relatively safe, but it is by no measure a guarantee. An adage I remember from what [one author and former vlogger](#) said, is that you can only be 100% private *if* you never left your home, never said anything, and consequently, never did anything, either. Obviously, this is patently ridiculous, but it serves to illustrate the *voluntariness* of anything you choose to say, and therefore it is important for you to be cognizant of so you can make informed decisions about what to do. The beauty of **keeping your own counsel** is that it encourages you to make conscientious decisions about [what you never say over the telephone](#), what you will say only privately, and what you may say publicly, if at all.

As a blogger, I realize that I am constantly walking a tight rope when it comes to INFOSEC, and it can be a very precarious balance at times. If you decide to go public about what was said during private conversations, then at the very least don't say whom you were talking to, because to do so otherwise would be a violation of their individual privacy. Not too long ago, I considered writing a tutorial on how to expose informants, but upon reflection, it dawned on me that such knowledge ought to be considered within the realm of INFOSEC.

Speaking of informants, snitching is the act of purposefully giving intelligence to the government. Snitches are dangerous because what they say to agents of the State usually gets people in serious trouble (like being fined, incarcerated, physically injured, or even executed). This is why an adage like "[snitches get stitches](#)" becomes socially acceptable, even by those *without* criminal records – the sheer danger of tattletelling to the police is so high that counter-cultural socialization reflects the condemnation of this behavior. If the use of "confidential informants" against political prisoners such as [William Wolf](#) and [Schuyler Barbeau](#) isn't enough proof for why snitching is repugnant to human liberty, then I don't know what else would be sufficient.

Aside from snitching, I think it is imperative to be aware regarding your own propensity to accidentally let private knowledge just "slip out" carelessly. Whether it be due to your habit of [talking to yourself out loud](#), or falling victim to a [social engineering hack](#), you must guard against letting yourself unwittingly assist hostiles in acquiring personally identifiable information. [Doxing](#) is but just one way that can be used to compromise INFOSEC; if you ever plan on conducting an armed resistance against the government, for example, then cache your guns somewhere, and keep your mouth tightly shut.

There will be times when you find yourself attempting to decide whether filling in application forms is worth the privacy trade-off. Consider leaving entire field entries blank, and fill them in only if the clerk or bureaucrat hands it back to you, instructing you to provide a specific piece of information. Letting your fear of being turned away empty-handed should not dictate that you act with unmitigated subservience to "[the powers that be](#)."

As the old World War II idiom goes, "[Loose lips sink ships](#)." To further reinforce this point, it could also be said that, "Fish are only caught because they open their mouths; keep yours shut," and, "If you keep your lips pressed together, the silly words won't fall out." I hope you can see how this disciplined practice of **keeping your own counsel** is also applicable as an entire way of life.

Section III:

Low-Profile Behavior

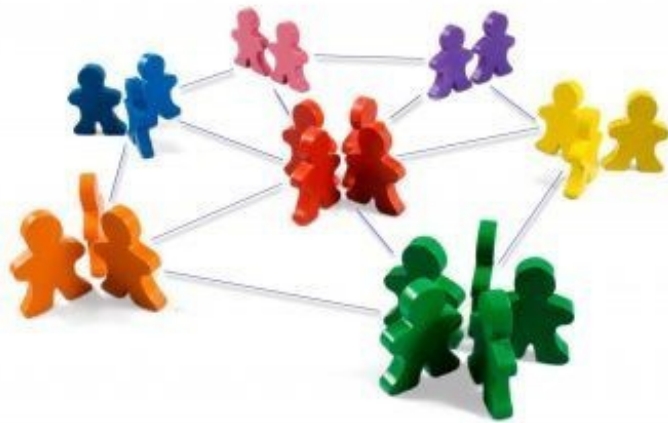
Chilling Dissent: How Government Demonizes Americans

 thelastbastille.wordpress.com/2015/05/11/chilling-dissent-how-government-demonizes-americans/

"First they came for the socialists, and I did not speak out, because I was not a socialist. Then they came for the trade unionists, and I did not speak out, because I was not a trade unionist. Then they came for the Jews, and I did not speak out, because I was not a Jew. Then they came for me, and there was no one left to speak out for me."

– [Martin Niemöller](#)

One of the most effective [propaganda](#) techniques is to manifest a [chilling effect](#) through the [demonization](#) of targeted individuals. [Chris Broughton](#) was originally cast by the mainstream media as an "angry racist protester," yet upon discovering he resembled Malcolm X noticeably more than Hal Turner, they had to change their portrayal of him to an "irresponsible gun owner." [Debra Medina](#) was initially hailed by the alternative media as the female incarnation of Ron Paul, yet when she tried to avoid explicitly supporting the 9/11 Truth movement, the Truthers and their ringleader, Alex Jones, cast her as a "flip-flopper" soon after her infamous interview with Glenn Beck, regardless of the fact that she was deliberately attempting to focus solely on Texan political issues instead of commingling them with national ones.



Statists favor the use of [censorship](#), [intimidation](#), [SLAPP lawsuits](#), and [malicious prosecutions](#) in order to stifle our common freedoms of [speech](#), [press](#), [assembly](#), and [petition](#), which are explicitly recognized by the several American constitutions. According to the [First](#) and [Tenth Amendments](#) to the United States Constitution of 1787:

"Congress shall make no law...abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

"The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

What this tells us is that the national legislature is clearly forbidden to enact any laws that violate the exercise of those liberties. Since we are also implicitly told by the Tenth Amendment to consider the relevant state constitution, let us now consult [Article I §§ 8, 27, & 29](#) under the Texas Constitution of 1876:

“Every person shall be at liberty to speak, write or publish his opinions on any subject, being responsible for the abuse of that privilege; and no law shall be passed curtailing the liberty of speech or of the press.”

“The citizens shall have the right, in a peaceable manner, to assemble together for their common good; and apply to those invested with the powers of government for redress of grievances or other purposes, by petition, address or remonstrance.”

“To guard against transgressions of the high powers herein delegated, we declare that everything in this ‘Bill of Rights’ is excepted out of the general powers of government, and shall forever remain inviolate, and all laws contrary thereto, or to the following provisions, shall be void.”

So, we have a constitutional situation here in America whereby expression of a man’s thoughts are considered sacrosanct in the law, and cannot be abridged or curtailed by either the U.S. Congress or the Texas Legislature. If men freely choose to collectively gather together in order to express themselves, that too is sacred, much like [the right to keep and bear arms](#).

The [Omnibus Crime Control & Safe Streets Act of 1968](#), aka, the “Wiretap Statute,” formed the bedrock statutory legislation for all intelligence on criminals. In 2001, both the [USA PATRIOT Act](#) and the [Aviation & Transportation Security Act](#) were passed; the former permitted the government to [warrantlessly search](#) bank statements, medical records, and even your [library borrowing history](#), whereas the latter created the now dreaded [Transportation Security Administration](#) (TSA). Following [Amerithrax](#), the [Homeland Security Act of 2002](#) gave more power to the [Office of Homeland Security](#) by “upgrading” it to the [Department of Homeland Security](#) (DHS), which is concomitantly headed by a [cabinet secretary](#). Thankfully, the [Violent Radicalization & Homegrown Terrorism Prevention Act of 2007](#) gloriously failed, although it shouldn’t be ignored that the Congress sincerely tried to criminalize so-called “[homegrown terrorism](#),” a term so vague at the time that its applicability would easily include those constitutionally recognized activities mentioned earlier.

Federal judicial case precedent is blatantly clear about the legality of personal expression, especially political free speech. The United States Supreme Court’s decision in [Brandenburg v. Ohio, 395 US 444 \(1969\)](#) explicitly spells out that mere discussion, [or even advocacy](#), of the people exercising their common [right of revolution](#) is constitutionally recognized political expression under the Free Speech and Free Press clauses within the First Amendment, with the only proviso being that said advocacy **not** threateningly identify any particular individual, and **not** [incite unlawful actions quickly](#). Now, although the *Brandenburg* decision should be a suitable defense against all charges of either [sedition or seditious libel](#), because of the lack of incitement, I am hesitant to say whether the case law would suggest it might work should a defendant be charged with [conspiracy](#).

Despite the constitutionality of political expression, the government willfully engages in pigeon-holing American dissidents for “[thought crimes](#)” by their political targeting campaigns through the use of

defamation, libel, and slander. The [copious documentation available to the press and the public](#) about the “intelligence” reports issued by the [fusion centers](#) unquestionably demonstrate the government’s ubiquitous attempts at criminalizing dissent primarily through [guilt by association](#), just as in a [police lineup](#). Law enforcement officers are brainwashed by [DHS’s scenario training](#), which encourages their paranoia about the American citizenry. Government police are deceived by the troves of misinformation that play on their inclination to fantasize about catching “the big one,” thereby making them highly susceptible to the [Jack Bauer Syndrome](#). The result of all this [government-sponsored defamation](#) is nothing less than the manifestation of a chilling effect through demonization.

Unjust dissident profiling and labeling is not only arbitrary, but also factually incorrect. Whether it be by way of profiling specific behavior as indicative of the “[signs of terrorism](#),” or the regular use of [fallacious arguments](#), the incessant portrayal of American dissidents as criminal malcontents is really beyond the pail. Anyone initially declared an “unlawful enemy combatant” by the Bush White House was legally considered to be so under § 948a(1) within the [Military Commissions Act of 2006](#), although this was meaninglessly changed to “unprivileged enemy belligerent” under § 948a(7) within the [Military Commissions Act of 2009](#), since both terms entailed “material support,” a concept that is ever expanding beyond its purported meaning, which was originally limited to jihadists.

Speaking of fallacious arguments, the government and their corporate partners appear to enjoy using the [ad hominem](#) and [straw man](#) fallacies without hesitation. The [constitutionalist patriot faction](#) is routinely labeled as “[anti-government](#),” despite their public advocacy for [restoring constitutional government](#) (that is, the early American republics within **these** United States). This same political faction is also regularly accused of being “[racist](#)” or “[racially supremacist](#),” despite the fact that there is nothing to suggest in what [Justices Miller and Moody wrote](#) in the 1872 *In Re Slaughter-House Cases* and 1908 *Twining v. New Jersey* decisions, respectively, that race is even relevant to [state citizenship](#) at all. Less common name-calling over the years has included, “radical,” “enabler,” and “tax rebel.”

Probably the most commonly used defamatory label used by [the State](#) these days is “extremist.” This is rather curious, for up until recently, the closest definition for “[extremism](#)” was that there was no objective definition, yet a [leaked Department of Defense military scenario training document](#) provided this definition:

“Extremism [is a] term used to describe the actions or ideologies of individuals or groups who take a political idea to its limits, regardless of unfortunate repercussions, and show intolerance toward all views other than their own.”

If I didn’t know any better, I’d suggest that the military’s definition of “extremism” describes the [GOP](#) and the so-called “[democrat](#)” political parties accurately, but I digress. Unfortunately, this is a tad problematic when you consider [that the Congressional Research Service described the term “extremist” as being deliberately vague](#) so that the government can enjoy prosecutorial flexibility in charging defendants for terroristic actions without having to formally charge them with actual terrorism. When Larken Rose, [an avowed anarchist](#), was [labeled an “extremist”](#) by a YouTube user who claimed he was a policeman, I’m sure you can begin to appreciate the seriousness of the mere accusation itself, although thankfully, [a joint intelligence bulletin by DHS and FBI](#) issued last month (on April 16th of 2015) finally defined, after all these years, what “domestic extremism” means:

*"Domestic extremism [is defined as] individuals present in the United States who seek to further political or social goals, wholly or in part, through unlawful acts of force or violence. The mere **advocacy** of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may **not** constitute extremism, and may be constitutionally protected." [emphasis added]*

How very revealing this newest definition is, isn't it? Suffice it to say, the government appears to be backpedaling by narrowing the definition after the fact, much like they did with "[terrorism](#)." So, according to the new DHS/FBI definition, not only does extremism necessarily require actual committed acts of violence, but also that the mere **advocacy** of such techniques is constitutionally recognized, presumably via the 1969 *Brandenburg* case. Should Larken Rose, as well as the patriot faction, be expecting apologies from the [Bureau of Justice Assistance](#) (BJA), the [Homeland Security Advisory Group](#), the [United States Coast Guard](#), the [Federal Protective Service](#), the [United States Military Academy at West Point](#), or [Demos](#), among other entities, for their systematic demonization of American political dissidents?

This begs the question, though, as to the role of civil disobedience, or perhaps, [civil defiance](#), in light of this newest understanding by what the federal government means by "extremism." Would [Saul Alinsky's radicals](#) be considered extremist? Alinsky is constantly mentioning throughout his primer about the "revolutionary organizers," yet I cannot find a black bloc keying cars or bashing in storefront windows anywhere in the text. Would [Gene Sharp's revolutionaries](#) be considered extremist? Again, it's not as if they are [shooting cops](#) anytime soon, so I'm going to assume that even calling them "revolutionaries" is intellectually dishonest. Fascinatingly enough, [the removal of the barricades](#) in front of the [World War II Memorial](#) during [the last government shutdown](#) by WWII veterans, as well as [the Cattle Unrustling a little over a year ago in Nevada](#), were "nonviolently" peaceful, despite the fact they were both acts of civil defiance.

Let us now examine a rather unique case study where said unjust government profiling was used to essentially [balkanize](#) and dismantle civic groups. For fiscal year 2012, the [New Hampshire Department of Safety](#) applied for a federal grant in the amount of \$258,024 for a [Lenco BearCat](#), which is literally an [armored personnel carrier](#). Within the application was this description of New Hampshire's "terrorism" problem:

"The State of New Hampshire's experience with terrorism slants primarily towards the domestic type. We are fortunate that our State has not been victimized from a mass casualty event from an international terrorism strike however on the domestic front, the threat is real and here. Groups such as the Sovereign Citizens, Free Staters, and Occupy New Hampshire are active and present daily challenges. Outside of the officially organized groups, there are several homegrown clusters that are anti-government and pose problems for law enforcement agencies."

This spurred justifiable outrage, such as the [Thanks But No Tanks](#) campaign, simply because the NH Department of Safety profiled the Occupiers, [sovereigns](#), and Free State Project (FSP) members as domestic terrorists, without *any* evidence or probable cause to sincerely believe *any* of them have

engaged in *any* criminal activity whatsoever. Once [Christopher Cantwell explained the rationale](#) as to why statists would want to use APCs against Free Staters, the [Free State Project Board of Trustees quickly purged him from their organization](#), without any consultation from the rank and file membership of the FSP. The subsequent fallout from this has been the adoption of the mainstream media term “[violence advocate](#),” by such alternative media outlets like [Free Talk Live \(FTL\)](#), to describe any political dissident who simply reminds the public at-large of their common right, [and even duty](#), of revolution. Ironically, this politically correct thought policing by the FSP and FTL directly contradicts not only [§ 627:4 of the New Hampshire Revised Statutes Annotated](#), but also [Articles 2-a & 10 within the New Hampshire Constitution of 1784](#), which say, respectively, that:

“All persons have the right to keep and bear arms in defense of themselves, their families, their property and the state.”

*“Government being instituted for the common benefit, protection, and security, of the whole community, and not for the private interest or emolument of any one man, family, or class of men; therefore, whenever the ends of government are perverted, and public liberty manifestly endangered, and all other means of redress are ineffectual, the people may, and of right ought to reform the old, or establish a new government. **The doctrine of nonresistance against arbitrary power, and oppression, is absurd, slavish, and destructive of the good and happiness of mankind.**” [emphasis added]*

As you can no doubt tell by now, this peacenik agenda by the FSP & FTL is rather, well, anti-libertarian, because these pacifists are using the [non sequitur fallacy](#) by insinuating [that self-defense implicitly endorses revolution](#). Individuals who live by the non-aggression principle understand that the deontological burden of proof is much higher for revolution than for self-defense, and the Texan equivalent of NH’s constitution and statutes on this matter lie in [Article I §§ 2 & 23](#) of the Texas Constitution and in the [Texas Penal Code §§ 9.31 – 9.33](#), especially [§ 9.31\(c\)](#). This ongoing attempt by the FSP & FTL to drive a wedge between libertarians and the patriots is nothing short of utterly disgusting; whether or not the FSP & FTL are [controlled opposition](#), or are just very useful idiots playing their role according to the [Hegelian Dialectic](#) formula, does not matter much, because I think the effects of this peacenik rhetoric speaks for itself in terms of chilling dissent, thereby doing the work of the State for them.

Alarming, the very accuracy of the government’s profiling of dissidents, whenever it’s not being deceptively vague, is always methodologically skewed. Fictional [predictive programming](#) elements, in movies like [Minority Report](#) or television shows like the anime [Psycho-Pass](#), give the impression that the government is [omniscient](#) because of its [precognitive](#) capabilities. This entire notion of “[precrime](#)” is a blatant abuse of *mens rea*, because it presumes that mere potential criminal intent, absent any criminal action, is sufficient for prosecution by the State. Actual criminal profiling is always done on an **individual** basis, not collectively (as DHS is [all too eager](#) and [fond of doing](#)) Actual profiling is very labor intensive in terms of gathering and sorting the evidence, and even then, [only specially trained profilers have any sort of real accuracy in constructing offender profiles](#), above and beyond that of the comparable accuracy of college students, psychologists, and even homicide detectives.

Unfortunately, it’s not just the State that is unjustly profiling dissidents, but also [non-governmental organizations](#) (NGOs) as well. [The Militia Watchdog](#) by the, ironically titled, [Anti-Defamation League](#) (who exist only to defame others), and [Meet the Patriots](#) by the [Southern Poverty Law Center \(SPLC\)](#), showcase

different [enemies lists](#) whose purpose is to illustrate specific examples of their political opposition. Personally, I have zero problems with the whole concept of drafting an enemies list [for other reasons](#); what I **do** have a problem with here is the fact that these NGOs are deliberately lying to the government about said dissidents in the blatantly obvious attempt to sic the [King's guards](#) upon all of them. The [SPLC itself is nothing more than a huge scam](#) that was begun by [Morris Dees](#) in the admitted attempt to make money by any means possible, as evidenced in part by locals in Montgomery, Alabama describing the SPLC's headquarters as the "[Poverty Palace](#)." Interestingly enough, it would seem as if the SPLC only backpedaled with regards to [their portrayal of Dr. Ben Carson](#), albeit half-heartedly. Bigotry, much?

Another key aspect of this whole mess is the government's insistence on "policy" over that of the law. Nearly everything, when it comes to [the notorious hoax that is the so-called Global War on Terror](#), is about "national security policy," not criminal law or even the Congress's [enumerated power](#) in granting [letters of marque and reprisal](#) to privateers in order to attack and capture these elusive "terrorists," just as if they were the [Barbary pirates](#) during the early American republic. Instead of following the legal remedies available to the Congress that are clearly enumerated in the federal Constitution, they have chosen instead to construct this elaborate illusion of [security theater](#) throughout much of the [federal bureaucracy](#) where due process is routinely denied and the malicious prosecution of individuals such as [Larry Myers](#), [Robert Beecher](#), and [Kevin Massey](#) is the "[new normal](#)," *not* the exception.

Some detractors at this point might question, why should they care if they or others are unjustly profiled by the government, presumptuously skeptical that these attempts at chilling dissent are only practically effective if they are actually enforced. Consider, for a moment, national defense projects such as [C3CM](#), or the TSA's [Screening of Passengers by Observation Techniques](#) (SPOT) [microexpressive](#) profiling method, the latter of which the Government Accountability Office (GAO) [recommended SPOT be scrapped](#). Those fusion centers with the inaccurate "intelligence" I mentioned earlier, which were [recommended by the 9/11 Commission](#) to facilitate "intelligence sharing," exist today in the form of the Texas Department of Public Safety's [Texas Fusion Center](#), which comes under the auspices of the [Regional Organized Crime Information Center](#) (ROCIC) that is one of the [Regional Information Sharing Systems](#) (RISS) administered by none other than the BJA, much to [the chagrin of religious clergy here in Texas](#).

Enforcement is not only limited to integrated databases and Stasi-styled behavioral detection police checkpoints. Police militarization includes not just the "armoring up" of officers, as evidenced by the earlier referenced BearCat case study, but also the use of [Visible Intermodal Prevention & Response](#) (VIPER) teams in [Tampa](#) and [Atlanta](#), the [dangerously violent midnight raids](#) to enforce narcotics prohibition, and the [military's treatment of protesting](#) as "[low-level terrorism](#)." Whether it's the [U.S. Army Reserve conducting surveillance on End the Fed protestors](#), or the [NYPD turning Pier 57 into a temporary concentration camp](#), the takeaway here is that the State has a multitude of enforcement options to use once they've profiled you as an American dissident.

Of course, the enforcement need not be as draconian as being killed by [drone strikes](#) like a Pakistani, simply because the government could just [blacklist](#) or incarcerate you on a whim. TSA's infamous No Fly List [has banned young children from flying on commercial jets](#), yet the No Fly List was also [promoted to become a No Gun Buy list by Rahm Emanuel](#) on the premise that your right to keep and bear arms should also be **canceled**, regardless of [the incompetent "mistakes" TSA gets routinely caught doing](#).

More insidious enforcement necessarily uses Soviet tactics to identify, search, and capture the politically undesirables in question. The [advanced imaging technology](#) TSA was using to scan the naked bodies of nearly all passengers, was just exploiting the airports as laboratory beta-testing, for what they want to use everywhere else with [the mobile x-ray scanners](#) and their [handheld equivalent](#). DHS's initial promotion of the [Future Attribute Screening Technology](#) (FAST) featured asking stupid questions about copyright

infringement while also using biometric facial recognition to scan the hapless citizen for behavioral clues of “malintent,” as if it were a high-tech version of TSA’s SPOT.

Those fusion centers, yet again, come back into play for their role in attempting to profile dissidents as being [gang members](#), pursuant to [Texas Code of Criminal Procedure Article 61.02](#), [Texas Penal Code § 71.01\(d\)](#), and even [28 CFR §§ 23.1 – 23.4](#), whose authorizing legislation was none other than the infamous 1968 Wiretap Statute, all of which was admitted by the [Texas DPS’ TXGANG database overview](#). Greenmail, much?

[Involuntary commitment](#) laws are still legal here in Texas, pursuant to [Article I § 15-a of the Texas Constitution](#), and the Texas Health & Safety Code [Ch. 573](#), [574](#), & [§ 571.020](#). If you express your political dissent on Facebook like [Brandon Raub](#) did, then just don’t be surprised when you get whisked away by the government police off to the American version of the [Psikhushka](#).

A few more thoughts on surveillance and enforcement before moving on to mitigation options. [Fake online users](#) hired by the government to [harass or entrap you](#) is only viable if you leave behind a noticeable [digital footprint](#). Efforts at [data-mining](#) your [voter files](#) or other [metadata](#) is useful only insofar as it increases the [predicative ability](#) of the government to [anticipate future trends accurately](#). As United States Attorney [Ann Tompkins](#) said [regarding Bernard von NotHaus’ Liberty Dollar](#) :

“Attempts to undermine the legitimate currency of this country are simply a unique form of domestic terrorism. While these forms of anti-government activities do not involve violence, they are every bit as insidious and represent a clear and present danger to the economic stability of this country. We are determined to meet these threats through infiltration, disruption, and dismantling of organizations which seek to challenge the legitimacy of our democratic form of government.”

Putting aside the very high degree of cognitive dissonance imposed by that very Orwellian and self-contradictory language by Tompkins, this is exactly what happens when lawyers use vague and ill-defined definitions for words like [“terrorism”](#). It is precisely because of this irrational blind obedience to illusory authority that has led to these ongoing attempts at chilling dissent.

How might it be possible to reign in these tyrannical excesses of government, which directly violate our freedoms of [speech](#), [press](#), [assembly](#), and [petition](#)? The answer to security theater is [security culture](#). Hard as it may be to hear, the fact of the matter is that due to the nature of our overall political situation, you and I might as well be [kulaks](#) in [Soviet Russia](#) or [Parisians](#) in [occupied France](#). Civil liberties are, quite frankly, a sick joke, so unless you find yourself in court, despite your attempts to avoid litigation using the tattered vestiges of American republicanism as part of your defense, [screaming bloody murder at the airport about constitutional infringements](#) will get you nowhere.

Many people have their own ideas about [how to make security culture work](#). For instance, [Bruce Schneier](#) has recommended thinking of security itself as a [trifecta of feelings, model, & reality](#), by which he means our emotional attitude, rational conception, and the objective facts regarding security, ideally bringing our emotions and concepts of security towards what is actually happening to us objectively. What I enjoy about Schneier’s trifecta is that I can extrapolate it out to mean that the government’s security theater is completely skewed because all of its feelings about [risks](#) are grossly disconnected from reality, besides

the fact that its models are based on feelings and not reason. This is why I believe security theater to be the polar opposite of security culture.

Security culture also entails the use of practical techniques for minimizing [threats](#) by [adversaries](#). [Aton Edwards](#) has counseled his audience to never underestimate the power of disinformation, by which he means using false information against your adversaries. For instance, driving an [inconspicuous car](#), or using other low-profile techniques, might just make the difference as to whether you are going to have to use the skills you've practiced from [role-playing police interrogations](#). Learning what the specific characteristics are that the [Missouri Information Analysis Center](#) (MIAC) and BJA are looking for in what they consider to be "[suspicious behavior](#)" or "[signs of terrorism](#)" will give you a leg up in determining whether you want to antagonize or avoid government police. Better yet, just [keeping your own counsel](#) and using believable [legends](#) will save you a lot of heartache.

An almost untouched upon element of using security culture in order to sidestep the chilling effect by the State is [the secured archival of one's records](#). Whether it be by way of encrypted online cloud storage or physical media such as an external hard disk, USB memory sticks, or burnable CDs & DVDs, the fact of the matter is that should your computers be seized or hacked into, you need mirrored spares of your most important files (probably with file encryption to boot). Chilling dissent can be something just as simple as coercively depriving you of your records through subpoena or seizure, so having both digital and paper copies of the same information, preferably in different locations, is definitely something to consider.

While most people could easily begin incorporating security culture into their own lives gradually, there is also a lifestyle choice you could make that is consistent with living [off-the-grid](#). The [vonu strategy](#) is the epitome of what some libertarians have called "[Going Galt](#)," where instead of willful apathy, you become purposefully invisible. Practitioners of this strategy believe that the best way to avoid being coerced is to remove yourself from all influences of coercion; this could be done by living in a semi-nomadic way, using mail drops, pseudonyms, crypto-currencies, bartering, or even as a [perpetual traveler](#), all the while abstaining from engaging in activities requiring licensure. [Tom Marshall](#) is usually credited with coining the term, and it would also appear that he began following his own advice ever since 1974, when he literally disappeared.

Heading off misconceptions before they rise, I'd like to point out that security culture is not limited to being a "lone wolf" affair by any means. Formulating an "[arrest plan](#)" entails having at least one person you implicitly trust on the outside who'd be your single point of contact should you need anything, such as access to the press. People interested in organizing along the lines of [leaderless resistance](#) must implement security culture for their [affinity group](#), regardless of whether such affinity takes the form of a [security team](#) or a [private defense agency](#). The reason why American patriots like [Kevin Massey](#) and [William Wolf](#) got persecuted by the federal government the way that they did is because they both had terrible security culture; if [monkey-wrenchers](#) can perform their operations successfully most of the time without getting caught, shouldn't we at least consider the possibility that they take security culture much more seriously than the patriot faction?

In order for the State's program of chilling dissent to work, they must identify, isolate, and eliminate perceived threats to their alleged legitimacy; what this means is that they cannot eliminate whom they cannot isolate, and they cannot isolate whom they cannot identify. Therefore, their tyrannical designs necessarily requires relentlessly undermining their attempts at identification. [As I have admitted before](#) on [at least a few occasions](#), the name "Kyle Rearden" is just my current [nome de plume](#), and in that respect is similar to [my previous alias](#). However, this is not just a pragmatic choice I made, but it is also a principled rejection of my legalized slave name, in much the same way [Malcolm X](#) did with his name. I mention this yet again only to stress the fact that if we all are to secure our liberties again, implementing privacy safeguards ought to be an indispensable element in order to avoid becoming susceptible to the

temptation of allowing our dissent to be chilled.

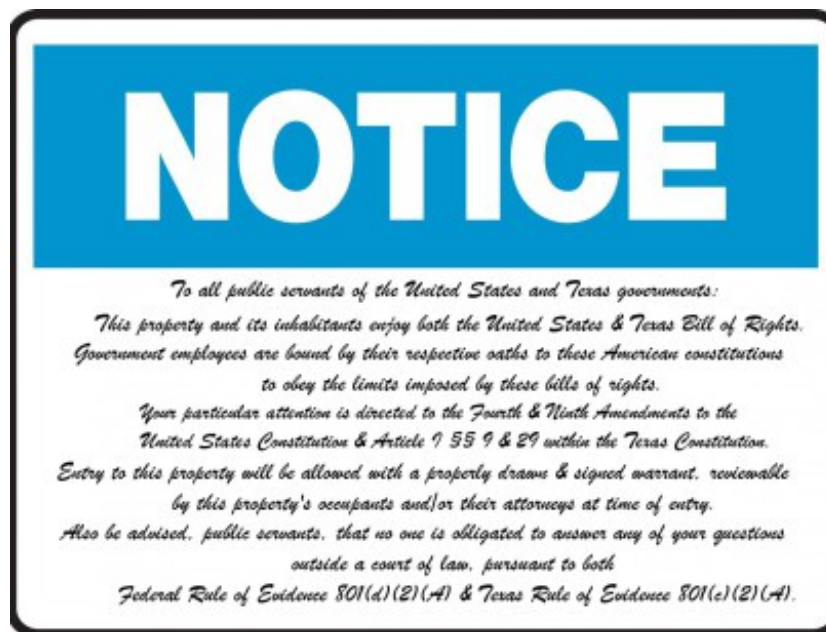
Postscript: *I'd like to extend a special thanks to Shane Radliff of [Liberty Under Attack](#) for graciously hosting all of the original source material I used in preparation for this article. Should you want to learn more nuanced details about how the government profiles dissenters, then I would encourage you to download and read all of the documents and videos from LUA's [profiling archive](#).*

Fanciful Notices: Should You Post a Warning Sign on Your Property?

www.thelastbastille.com/2016/03/08/fanciful-notices-should-you-post-a-warning-sign-on-your-property/

"The right to privacy comes from 'Thou shalt not steal.' I don't want you to steal from me and I'll bet that you don't want me stealing from you, so I think you probably agree with me that it's a desirable law. 'Thou shalt not steal' is the basis of property and property rights, and privacy is incident to property. Privacy and property go together like a pilot fish suckered on a shark. If you want privacy, you have to have property rights."

— The Anti-Terrorist



During the early morning hours, the family dog can be heard barking unusually loudly, until he is permanently silenced by a quiet attacker. Suddenly, a boot crashes through your front door, and a dozen [armed men clothed in black rush throughout your entire home](#) pointing automatic weapons at everyone in your household. Yelling, shrieking, and flash bangs are the sounds that greet you as you awkwardly jerk from your slumber.

Whether it be due to [growing cannabis](#) or [homeschooling](#) your children, [the State](#) will use whatever (flimsy?) pretext by which to literally invade your life. Seriously disrupting your lifestyle by grinding everything to a screeching halt is what Leviathan excels at doing. The only question at this point is, considering the fact that [America is a police state](#), what can be done to prepare for such an event?

Some have suggested investing in custom aluminum warning signs that describe what the government's own laws say with regards to search warrants. What is being presumed here is that when the police officers who executed the warrant are testifying later in court, they will be compelled to admit, under penalty of perjury, that they saw your warning sign, and instead of approaching you like civilized men, they decided to raid the joint like a gang of well-armed thugs; it is further assumed that by doing so, they will be conceding a favorable court decision to you that will end up curtailing the power of government, or at the very least, getting you financial recompense for your endurance

of the whole ordeal. Although this tentatively sounds like an intriguing idea, in reality the actual exercise of carrying this out presents noticeable obstacles in terms of its efficacy.

For instance, an aluminum sign costs quite a bit more than a rigid plastic one [by a factor of between one & one and a half times](#). Rounded corners cost somewhat more, but the range of the ratio is still about the same, even though it costs about \$5 more in order to [not have sharp corners that can cut you when mishandled](#). Generally speaking, for custom aluminum signs in 12 x 6" dimensions, you're looking at \$20 – \$25; in 24 x 12", it's more like \$30 – 40. Obviously, if you're getting more than one sign, then just multiply the estimated cost range by how many you want; for example, if you want two signs in 12 x 6", you're looking at \$40 – \$45, whereas a set of **four** signs in 24 x 12" will be roughly \$120 – 160. As can be expected, it's cheaper buying one or two signs for your external doors (even in a larger size) than it would be getting multiple signs, in almost any size, for different points along your fence, including the gate.

Unfortunately, such a monetary investment in this kind of warning sign is the antithesis of the [grey man](#). Much like [bumper stickers on your car](#), these warning signs, whether they be on the front door or the gate to your property, call attention to yourself as someone who is (falsely) perceived to want to "[police the police](#)." At best, you'd be loud and proud in a rural area, but in a suburban or urban setting, warning signs really only serve as an undesirable [target identifier](#); this is especially pronounced if you live in an apartment, as opposed to a house.

Constitutionally, the federal and Texas governments have clauses relating to warrants as well as searches and seizures. The [Fourth](#) and [Ninth](#) Amendments to the [United States Constitution](#) and [Article I §§ 9 & 29 within the Texas Constitution](#) say, respectively, that:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

"The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

"The people shall be secure in their persons, houses, papers and possessions, from all unreasonable seizures or searches, and no warrant to search any place, or to seize any person or thing, shall issue without describing them as near as may be, nor without probable cause, supported by oath or affirmation."

"To guard against transgressions of the high powers herein delegated, we declare that everything in this 'Bill of Rights' is excepted out of the general powers of government, and shall forever remain inviolate, and all laws contrary thereto, or to the following provisions, shall be void."

In other words, both governments claim to value the right to privacy implicitly, as the only legal exception to this is when they are investigating crimes, and even then, they are hypothetical "[limited](#)" to what they can do, hence the warrant clauses found in both constitutions. Reality, however, testifies to a wholly dissimilar conclusion, at least with regards to the [history of dragnet wiretapping](#) by the *federal* government.

Given that there are [two classes of American citizenship](#), perhaps [jurisdictional arbitrage](#) can be leveraged here in order to gauge the likelihood of securing a legal victory against the government for [color of law](#) violations. According

“Whoever, under color of any law, statute, ordinance, regulation, or custom, willfully subjects any person in any State, Territory, Commonwealth, Possession, or District to the deprivation of any rights, privileges, or immunities secured or protected by the Constitution or laws of the United States, or to different punishments, pains, or penalties, on account of such person being an alien, or by reason of his color, or race, that are prescribed for the punishment of citizens, shall be fined under this title or imprisoned not more than one year, or both; and if bodily injury results from the acts committed in violation of this section or if such acts include the use, attempted use, or threatened use of a dangerous weapon, explosives, or fire, shall be fined under this title or imprisoned not more than ten years, or both; and if death results from the acts committed in violation of this section or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill, shall be fined under this title, or imprisoned for any term of years or for life, or both, or may be sentenced to death.”

In other words, if you violate someone’s rights under color of law, you could be fined and jailed for not longer than one year, but if there is a threat or actual injury resulting from such violation, you’d be fined and incarcerated for up to a decade; if you go further by attempting to kidnap, rape, or kill under color of law, then you’d be fined *and* rotting away your life in prison *or* suffering the death penalty, as all are on the table (some may also cite [42 USC §§ 1997a & 14141](#), but these only deal with the Attorney General having grounds to sue based upon the rights of the “institutionalized” generally, or juveniles specifically, being violated, respectively). By contrast, [Texas Penal Code § 39.03](#) says:

(a) A public servant acting under color of his office or employment commits an offense if he:

- 1. intentionally subjects another to mistreatment or to arrest, detention, search, seizure, dispossession, assessment, or lien that he knows is unlawful;*
- 2. intentionally denies or impedes another in the exercise or enjoyment of any right, privilege, power, or immunity, knowing his conduct is unlawful; or*
- 3. intentionally subjects another to sexual harassment.*

(b) For purposes of this section, a public servant acts under color of his office or employment if he acts or purports to act in an official capacity or takes advantage of such actual or purported capacity.

(c) In this section, “sexual harassment” means unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct of a sexual nature, submission to which is made a term or condition of a person’s exercise or enjoyment of any right, privilege, power, or immunity, either explicitly or implicitly.

(d) An offense under this section is a Class A misdemeanor, except that an offense is a felony of the third degree if the public servant acted with the intent to impair the accuracy of data reported to the Texas Education Agency through the Public Education Information Management System (PEIMS) described by Section 42.006, Education Code, under a law requiring that reporting.

Put another way, what would be punished more harshly by the feds is, presumably, in Texas, usually just a Class A misdemeanor, which according to [§ 12.21 of the Penal Code](#), is only a maximum penalty of a \$4,000 fine and one year in jail. Interestingly enough, [what else is considered a Class A misdemeanor in Texas?](#) Well, victimless crimes like selling liquor on Sundays, selling beer on Sundays before noon, openly carrying a handgun *without* a license, *repeated* prostitution or pimping, desecrating either the Old Glory or Lone Star flags by burning, disorderly conduct, possession of cannabis between 2 – 4 ounces, possession of “drug paraphernalia” with “intent to deliver,” resisting arrest, failure to appear (that is, bail-jumping), and my personal favorite, escaping *unlawful* custody.

Imagine, if you will, a SWAT team were executing a search warrant, and that warrant was proven to be defective in court, as well as the fact that the police officers were found guilty **by a jury** to be acting under color of law in serving the defective warrant – then statutorily, [felony convictions would be on the table](#) if the case was being tried in federal court, but if it was under the jurisdiction of Texas, then it would only be a misdemeanor, from what I can tell. Codifying in statutory law what is described by them as **official oppression** as only being as serious as selling liquor during “unapproved” times, or possessing cannabis in “unapproved” amounts, really only demonstrates the trivial attitude the Texas government appears to have towards their own employees and agents acting under color of law. Not that the feds are much better, for the FBI admitted that there were only [72 indictments in 2014 for color of law violations](#), nevermind *convictions*.

What about [suing the government](#), instead? Some might think that rather than filing a criminal complaint with [any Texas county attorney](#) or the [Offices of the United States Attorneys](#) in order to prosecute illegal SWAT raids, it'd be more effective to approach any sort of litigation through civil remedies, strategically speaking. I think the [seven different civil court cases of varying jurisdictions between 2007 – 2015](#) I've examined reveal the counter-productiveness of initiating lawsuits, at least within that sample. Regarding Texas specifically, the [Civil Practice & Remedies Code §§ 9.011 & 11.054](#) already present some hurdles that *pro se* litigants will likely have to contend with, whether it be demonstrating that they are not engaging in “groundless pleadings” (such as those in bad faith) or being found as a “vexatious litigant” who is then required to furnish a security – any failure to pony up some cash is grounds for dismissal of the lawsuit.

If you do decide to invest in a warning sign for your property as a way to “[hedge your bets](#)” as it were, what should it say? This is more of a matter of personal taste, not to mention being dependent upon which American legal jurisdictions are applicable to you, but I would venture a guess that the following phrasing **might** apply to Texans (as shown on this article's companion picture):

NOTICE

To all public servants of the United States and Texas governments:

This property and its inhabitants enjoy both the United States & Texas Bill of Rights.

Government employees are bound by their respective oaths to these American constitutions to obey the limits imposed by these bills of rights.

Your particular attention is directed to the Fourth & Ninth Amendments to the

United States Constitution & Article I §§ 9 & 29 within the Texas Constitution.

Entry to this property will be allowed with a properly drawn & signed warrant, reviewable by this property's occupants and/or their attorneys at time of entry.

Also, be advised, public servants, that no one is obligated to answer any of your questions outside a court of law, pursuant to both

[Federal Rule of Evidence 801\(d\)\(2\)\(A\)](#) & [Texas Rule of Evidence 801\(c\)\(2\)\(A\)](#).

Obviously, feel free to substitute Texas (as well as the constitutional and evidentiary references) for wherever you live, but if this purported method of using a warning sign had any efficacy at all, this is approximately the wording I'd like to squish in there, if at all possible. I doubt that if a police officer on a SWAT team would testify under cross-examination that he took the time to read the warning sign, and then disregarded it via color of law by conducting the raid anyway. Not only that, but considering the different types of [exceptions to the warrant clause](#), I'm pretty sure that all any police officer has to do is convince the jury that any potentially defective warrant wasn't required anyway, and if he's persuasive enough, he'll walk away clean without being convicted and punished for acting under color of law, thus rendering warning signs moot.

While I am certainly a fan of [legal opportunism](#) whenever there is a chance to exploit loopholes in order to increase American liberty, I think there are better alternatives to warning signs that don't compromise security culture. [Role-playing police interrogations](#) would be my first recommendation, followed closely by formulating an [arrest plan](#). The main idea here is to learn and practice [refusing consent](#) and [keeping your own counsel](#) until it becomes second nature.

Although originally touted as a security culture technique, in reality, this advocacy for investing in custom aluminum warning signage is quite an exercise in [wishful thinking](#). Warning signs haven't satisfied [Hitchens' razor](#), given that I am unable to find any court cases that have been successfully litigated where the presence of warning signage made the difference in favor of the homeowner. Once you understand that [the law is a racket](#), then you can redouble your efforts in seeking more plausible options for restoring liberty.

How to Roleplay a Police Interrogation

 [thelastbastille.wordpress.com /2014/08/10/how-to-roleplay-a-police-interrogation/](https://thelastbastille.wordpress.com/2014/08/10/how-to-roleplay-a-police-interrogation/)

As the cancer of Big Government exponentially increases, so too does the frequency of direct contact with its employees. Whether that contact occurs in the form of a traffic stop, an airport security checkpoint, or as an armed raid on your home, deliberately avoiding the police as a way of life is not sufficient anymore in preserving whatever scraps of freedom you have left. Therefore, the most useful political skill any American can learn is how to successfully navigate the labyrinth of a police interrogation, with the singular goal of emerging from it as minimally harmed as possible.

Larken Rose was absolutely correct when he predicted that [the most common response he'd receive from the public](#) towards his question of [When Should You Shoot a Cop?](#) revealed most alarmingly just to what lengths many taxpayers will go to justify the initiation of violence by police against their fellow citizens. These cop groupies have [openly advocated for the theft, kidnapping, and even murder of anyone](#) who politely suggests that American citizens still retain their [natural right of self-defense](#), even against [those men who wear blue costumes adorned with shiny jewelry](#). I mention this only to illustrate the depth of [indoctrination](#) and [social conditioning](#) these propagandized individuals have been subjected to since their earliest years, besides my contention that it would be reasonable to infer that these cop groupies would also be predisposed to be the same people that, when serving as jurors, will tend to lend more credence towards anything a police officer says rather than any [exculpatory evidence](#) presented in court.



Remember the second sentence from the [Miranda warning](#)?:

| *"Anything you say can and will be used against you in a court of law."*

Well, if that's true, then let's extrapolate a bit here. If you say a lot, a lot can be used against you; if you say little, then little can be used against you. Thus, if you say nothing, then nothing can be used against you; so, it would make sense to say as little as possible, if anything at all.

What you are dealing with here in your encounters with the police is essentially a legalistic flytrap. Talking to the police automatically creates an expert witness against you, and [anything you tell them cannot be used as exculpatory](#), usually because of how the rules of evidence are written. Both [Federal Rule of Evidence 801\(d\)\(2\)\(A\)](#) & [Texas Rule of Evidence 801\(e\)\(2\)\(A\)](#) say:

| “A statement is not hearsay if the statement is offered against a party and is the party’s own statement, in either an individual or a representative capacity.”

This is precisely why it’s the wisest course to say nothing, deny nothing, and give them nothing to work with; it’s also the same reason why it is utterly foolish to make statements, no matter how innocent they appear. Remember the following adage:

| “The master asks the questions, and the servant answers them.”

Are you the master or the servant during a police encounter? This question is answered by your own behavior, so act accordingly. If you remember nothing else, then remember to *never make statements, and only ask questions*. Rephrase your statements in the form of a question if you must, but never admit to anything, if you can help it (I understand this is rather difficult if the questions posed to you are seemingly innocuous ones, such as during a traffic stop when the officer is asking whether the address on your driver’s license is your current one, but if you do answer such questions, keep in mind he is also trying to get a baseline reading on you, which he could use later during the encounter to manipulate you).

Why should you learn how to handle yourself during a police interrogation at all? Law enforcement officers are neither your friend nor your enemy, necessarily, but rather your adversary, much like an opponent who wants to “win” a situation, as if it were a game (albeit, a rather serious one). Police enjoy the sanctioned ability to infringe on your freedom by tricking you into waiving your liberties, typically by relying on your ignorance of them.

Asserting your **civil** rights is a form of insurance. Should you genuinely be culpable for some action you committed, then perhaps the extent of your punishment could be mitigated somewhat. Even if you presume you’re totally innocent, politely yet firmly asserting those rights acts as a legal shield that could help you, whether immediately on the street or later in court (this is assuming, of course, that the judiciary bothers to follow the limitations imposed by the applicable constitution and jurisdictional venue governing your case).

Despite the legal maxim that *ignorantia juris non excusat*, not even the cops themselves know what the laws comprehensively say, which is why they rely on [the lawyers](#). Officers rely solely on their police training while they go about enforcing the law. Therefore, in order to preserve your own freedom, keep yourself focused on task, namely, refusing searches, confessing nothing, and asking whether you are free to leave in peace.

Some people erroneously believe that the techniques of resisting interrogation many guerrillas train for are ineffective and a waste of time for the average civilian. Jan Karski, an operative for the Polish Underground during World War II, explained in his autobiography, [Story of a Secret State](#), how the actual practice of surviving the National Socialist occupation favored (perhaps counter-intuitively), on average, Polish partisans rather than the average Polish citizen. Karski said:

"In June 1940, the Germans staged a manhunt in the streets of Warsaw and seized about twenty thousand people who were taken to three large police stations where they were searched, questioned, and had their documents verified...[a]ll those whose documents were not in perfect order, who could not give a satisfactory account of their ancestry, employment, and political sympathies, or could not clear themselves of charges made against them, were sent to concentration camps...[w]e later learned that about one hundred members of the Underground were caught in this raid. They were, without a single exception, promptly released. Every one of those had his documents in perfect order, could prove his occupation, and supply a satisfactory account of his personal history. Every one had ready answers to every question that were asked of him and impressed the police by his clear, straightforward, and unhesitating manner."

Notice how those individuals who had *prepared* ahead of time to deal with the police were the best able to mitigate any harm that could be levied against them. The lesson to take away from this is that even if you are not an American political dissident of any kind, it would still serve your own self-interest to learn how to handle yourself during a police encounter. Just because you may be a sycophantic statist does not therefore mean you automatically enjoy immunity from prosecution, because, quite frankly, *everyone* is a potential target for harassment by *any* LEO, at *any* time, for *any* reason.

Why can role-playing police interrogations train you to better navigate the quagmire of an actual encounter? Simply giving you formulas is a necessary yet insufficient preparation, because without a working knowledge on how to *apply* those formulas to a variety of circumstances, such formulas might as well be strictly theoretical instead of also being practical. The idea behind role-playing is to take abstract concepts and make them as realistically concrete as possible, because that is where the true understanding actually takes place. A fabricated experience is still better than a classroom lecture any day of the week.

To get an initial idea on how role-playing these encounters are to be conducted, you may wish to watch [the workshop seminar the East Atlanta Copwatch put on last year](#), or the more [scripted scenarios presented by FlexYourRights](#). Pay attention to how they conduct debriefs of each scenario, and then redo each one, this time avoiding all the mistakes while performing the actions that best asserts their rights. Reliable formulas I've seen repeated in these and other similar role-player training videos are:

- Project a calm demeanor
- Never consent to any searches
- Determine if you are being detained, under arrest, or are free to go.
- Alternate between asking questions and being silent in response to questions.
- Don't run.
- Never lie to the officer, even inadvertently.
- Don't physically touch the officer.
- [Lawyer-up](#)

In accordance with these behavioral guidelines, there are what some call “magic words” you should use, depending on how the interrogation is proceeding. A sample include:

- “Am I being detained?”
- “Am I under arrest?”
- “Am I free to go?”
- “What is the nature of the intended detention?”
- “What crime am I suspected of having committed?”
- “Who accuses me of committing a crime?”
- “Officer, what is your probable cause that I may have committed a crime?”
- “Am I obligated to tell you that?”
- “Is that an order?”
- “Officer, I do not consent to any searches.”
- “I have nothing to say.”
- “I wish to have an attorney present during all further questioning.”

The last three are really the only valid exceptions to the adage I mentioned earlier, because refusing consent, remaining silent, and lawyering up are all civil rights that too many people recklessly waive that would have otherwise, more likely than not, have made the difference between having a criminal record and not having one (or at least, a less severe one).

How does one go about role-playing a police interrogation? At the very minimum, you need one other person who is willing to role-play with you. Props and costumes are helpful in establishing roles, as are verbiage, tone of voice, and body language. Although it is preferable to conduct such role-playing in person, it is also possible to do so only audibly, such as by telephone or VoIP (which negates body language and eye contact, but focuses more on vocal tremors and linguistic content).

What are the “rules of engagement” during such role-playing? The two principle role-players are the **Gendarmerie Cop** and **Joe (or Jane) Civilian**; the goal of the Gendarmerie Cop is to get Joe Civilian to admit to doing something “illegal,” whereas the goal of Joe Civilian is to survive the interrogation without confessing. The Gendarmerie Cop may physically intimidate Joe Civilian (such as by shining a light in his face, closing bodily distance, or raising his voice), but he is *never* allowed to physically touch Joe Civilian (no shoving, frisking, or tackling); this is done for the common sense safety of both role-players (besides, actual cops manhandle enough innocent people as it is). Joe Civilian scores “points” for not giving out any personal information (such as his full legal name, physical or mailing address, Social Security number, or any alibi); by contrast, Joe Civilian gets “demerits” if he lies to the Gendarmerie Cop.

Role-players should brainstorm a variety of scenarios, drafting them up ahead of time (as needed), and letting the individual who’s playing the cop for that particular round decide the situational context for the encounter. Agree on a [safe word](#) ahead of time to pause the role-play, just in case of an unavoidable interruption (but not for the sake of the civilian role-player becoming uncomfortable, because acclimatizing to the emotional pressure is one of the chief reasons for role-playing police interrogations in the first place). Always hold a post-roleplay debriefing and discuss what was learned, as well as what was done right and wrong by everybody involved in the scenario.

More advanced interrogation role-playing should at least include 2 or 3 Gendarmerie Cops trying to trip up Joe Civilian, if not also more serious charges looming over the civilian's head, more aggressively despotic cop tactics, or even the addition of another civilian to introduce a [prisoner's dilemma](#) element to the scenario. I remember a few years back when I and a few other guys were role-playing via VoIP, and we were taking turns being cops and civilians. One scenario's locale was at a police station, where I was getting double-teamed by two cops, ostensibly at first for what they seemed to be implying that I was aiding and abetting, which was then quickly escalated into concealment of evidence. My fellow role-players decided to up the ante by then insinuating that because they had an eyewitness who claimed I had been visibly angry at a woman I didn't know who was currently recovering in the local hospital, as well as the call log from the beaten woman's cellular telephone, that I was looking at a potential attempted murder charge if I didn't start "cooperating" with their investigation! Needless to say, I stuck to my guns, and after another several minutes of relentless questioning, my buddies ended the scenario by telling me I was cleared of all suspicion; everyone else who was part of the conference call that evening congratulated me on a job well done.

I would like to take a moment here and acknowledge the indispensable contributions made by the modern [state citizens](#) when it came to their innovative approaches to handling police encounters. Believe it or not, it was these state citizens who were, to my knowledge, among the very first political dissidents to create, develop, and refine the techniques and strategies for how to deal with the cops, which (ironically) for them was really more as a stepping stone to litigating in court. It wasn't until other people came along and focused solely on police interrogations did role-playing become as popular as it is today.

In addition to role-playing police interrogations, it couldn't hurt for you to learn some [rudimentary negotiation skills](#). A collection of Michael Gibson's simulations are featured on Newgrounds that are [free to play](#), besides the other free demos on ZAP Dramatic (if you were willing, you could also pay [a nominal membership fee](#) to play the entire archive). Should you be interested, there are also [free demos](#) of Gibson's otherwise \$300 online negotiation course you may want to try out before making a decision on whether to invest in it. Granted, although most of Gibson's simulations are not in the context of a police encounter, I see no reason why some of the tactics you learned from the other negotiation scenarios couldn't be transferred over or otherwise incorporated into your role-playing repertoire, as appropriate.

Two other tools deserve mentioning here. One is a digital *audio* recorder, for reasons [I have written about before](#), and the other would be the infamous "[Assert Your Rights](#)" card. Although some have recommended taping role-players as an educational tool with which to review their performance, I'm a bit hesitant to suggest the same for three reasons; namely, its true educational value, its function as a prop, and the likely potential for abuse, even if only inadvertent. The whole point of role-playing police interrogations is to do so *live* and *in the moment*, and the debriefs are done the same way only for the benefit of the participants; records are only necessary if you need some evidence of proving something in the *future* (and as a prop, you could substitute a different object and use sound effects). Besides the technical considerations of download, printing, and laminating a Fifth Amendment card, what is the point of role-playing police interrogations if all you have to do is hand a "magical" card over to the officer? My advice is for you to treat your digital audio recorder the same as you would a firearm, and only rely on the Assert Your Rights card more as a last minute refresher *before* the interrogation actually begins rather than as a flimsy backup should other techniques backfire.

Police encounters are downright scary, and almost nothing can truly prepare you for the throbbing in your ears or the shortness of breath you will likely experience. You are coming face-to-face with a [socialized mercenary](#) who literally holds the coercive power of life and death in his hands, so such an interrogation is not to be taken lightly or rushed. Only by coming to terms with this tyranny by realizing it can very much reach out and touch you are you truly ready to begin dealing with it as a [responsible adult](#). If you can't do something as basic as surviving a police encounter relatively unscathed, then you have no business

litigating *pro se* in court, either. The more you act as the “grey man,” the better off you’ll be; keep in mind too that police are legally permitted to lie to suspects, but the reverse situation is considered a criminal offense as a [false statement](#). I’ll leave you with what Officer George Bruch of the Virginia Beach Police Department [told a law school class several years ago](#):

“When I record a confession or an interview, because we don’t do interrogations, the police, we do not do interrogations. That’s a bad, mean, Nazi kinda word, ok? We do interviews. You’d be amazed how much difference it makes when you use that one word versus interrogation.”

Blending In: The Art of the Grey Man

www.thelastbastille.com/2016/01/13/blending-art-grey-man/

"The art of psychological disguise, on the other hand, lies in making oneself 'invisible' in a particular situation. The disguise artist develops the chameleonlike ability to blend into his surroundings so well that he cannot be seen as a separate entity. Just as a chameleon is perceived as being part of a pattern of leaves and twigs, so the disguise artist is perceived as being part of the pattern of a busy city street. The best disguise, as we shall see, does not always require a costume."

– Edmond McInaugh



Given the fact that American dissidents are [unjustly profiled](#) by the government, it stands to reason that [direct action](#) must be taken to stymie the [creation of political prisoners](#). Whether these injustices are due to malice or stupidity, the fact of the matter is that [the answer to security theater is security culture](#), and the foundational basis for security culture is the practice of being a grey man. A ["grey man"](#) is defined as:

"A man who can blend in to any scene or situation without standing out, hiding his skills and qualities."

Self-evidently, acting as a grey man naturally includes women, although to be sure, there are noticeable differences when it comes to physical appearances (especially fashion). The following description of the grey man was posted on the [Western Rifle Shooters Association](#)'s blog:

"The Grey Man is totally aware of his environs, his own capabilities or lack thereof, his weaponry and his levels of competence with that weaponry...the Grey Man NEVER draws attention to himself by word, dress, action, or mannerism...the Grey Man is a private man...the Grey Man goes far out of his way never to offend anyone, imitating the duck which appears calm on the surface on his pond whilst paddling like hell under the surface."

This imagery of what could arguably be the "[grey duck](#)" is quite a useful analogy in teaching others about this unique practice. [Pat Henry](#) has written that he thought the grey man was originally developed as a conceptual tool for [concealed carry practitioners](#), despite the fact that getting a license, or permit, for carrying concealed actually violates [information security](#) (INFOSEC) because such government lists also operate as a *de facto* registry of these gun owners, but I digress; the result has been the development of a method for practicing an evasive skill set.

The characteristics of the grey man are fundamental towards understanding how to pick it up and use it, just like any other tool. These four elements are:

1. Appearance
2. Behavior
3. [Situational awareness](#)
4. [Everyday carry](#)

Obviously, each one deserves its own cursory examination; the briefest yet comprehensive overview I can provide of these elements is that, how other humans perceive you greatly depends upon your ability to become nothing more than a stereotype. In this sense, the grey man runs counter to any notion of [individuality](#); however, the goal of the grey man is not to make friends or seek personal authenticity, but rather, to lower the existential risk of being targeted by [the State](#) and other assorted criminals.

Adversaries who perceive you as a soft target, due chiefly to your appearance, suggests you committed a mistake somewhere. Wearing clothing with logos is, generally speaking, a "no-no;" for example, decorative T-shirts worn by [sheepdogs](#) and [Three Percenters](#) (such as the infamous "[Tapout](#)" shirts), serve as little more than target identifiers. Tattoos are much like the [bumper stickers on your car](#) in that the temptation of vanity directly interferes with "going grey." Suffice it to say, neglecting the tips presented by [John Sample](#) with regards to making fashion choices is to invite failure to blend into the cultural environment.

Distinguishing the line between appearance and behavior is not as sharp and defined as you would initially assume. [Back in 1995](#), James Bovard was evicted from the press section of the [United States Supreme Court's courtroom](#) during oral arguments for the [Bennis v. Michigan](#) [516 U.S. 442] [civil asset forfeiture](#) case, simply because [he laughed too loudly](#), although the "official" reason was that he was inadvertently violating the dress code. Whether it be due to appearance or behavior (or both), Bovard's experience is invaluable for demonstrating that when you go visit the government, discretion really is the better part of

valor.

Undoubtedly, behavior is more significant to being a grey man than appearance. Quick movements naturally draws the attention of the eye, so even if you feel indescribable pressure to walk quicker, try hard not to; this may sound rather counter-intuitive, but if you truly want to be the grey man, then slower is better. [Political fieldtrips](#) are excellent opportunities to practice going grey, as are other public locales such as gyms and shopping malls. Dense congregations are the ideal training environment, given the sheer complexity of all the variables at play. For some people, it may be best to begin objectively evaluating their behavior by [recording themselves on camera](#) at home, and then later watching the footage for clues as to what their body language might be, perhaps inadvertently, communicating to others, [especially through their facial expressions](#).

Knowing that you are being indiscriminately surveillanced in public by officers and cameras, the challenge of the grey man is to maintain a rather drab persona all the while resisting the enticement to alter his behavior under pressure. Avoid establishing patterns – sometimes, it is best to just wait patiently rather than go somewhere right away, especially if doing so would get you noticed (or worse, if it's a trap); don't be afraid to choose different routes while traveling, and also consider the *frequency* of appearing in certain locations or within the eyesight of particular individuals. [Swiveling one's head](#) in order to look around might as well be the human equivalent to when a whitetail deer flips his tail up, for the latter serves as an instinctive warning to other nearby deer; instead, practice moving only your eyes when keeping tabs on fluid social dynamics.

Just as important to your behavior as movement, is what comes out of your mouth. [Keeping your own counsel](#) might as well be a given as this point, yet its importance for going grey cannot be overemphasized. Low-profile techniques include the use of [small talk](#), especially for making [non-committal](#) statements during casually polite questioning. The Italian idea of a “[nonchalant expertise](#)” is a good notion to aim for, since there is absolutely nothing illegal about acting as bland and dull a person as possible.

[Situational awareness](#) is nothing more intriguing than humble [mindfulness](#). Being presently in the moment is an essential attribute of the grey man, for it is this, more than anything else, that truly distinguishes him from the distracted mainline public. [Focused concentration](#) is indispensable for going grey, since you have to balance your body language (like your walking cadence and frequency of eye contact) with noticing passing details. Not only has [Kim's Game](#) been used to improve one's memory, but it also reinforces the fact that lackadaisical observation increases the sheer amount of missed clues present within the environment.

It has been broached within “prepping” circles that [being a grey man can become useful during emergencies](#), such as SHTF scenarios, but I think these [credit card preppers](#) greatly underestimate the value of acting like a grey man in the here and now. Sure, the value of subtly could make the difference between getting hurt or killed, yet, I would argue that the grey man's best utility is *before* there are infrastructure breakdowns, and this is further supported by the phases mentioned in [The Grey Man Directive](#). There is no good reason why non-survivalists cannot also practice being grey men, since going grey is more of a class of privacy techniques rather than something limited to mere survival methodology.

Having said that, [everyday carry](#) (EDC) is very much part of the grey man's repertoire, for it is comprised of his physical tool kit that he subtly keeps on his own person. Generally speaking, your EDC is going to be composed of what could be thought of as “[first line gear](#),” in order to distinguish it from, say, your fighting load or [bug out bag](#) (BOB). Much [survivalist media](#) over the years has explored the question of [what should or ought to be carried](#), whether it be for EDC, a BOB, or anything else.

I'd suggest that instead of focusing on specific pieces of equipment (as [gearheads](#) are all too eager and fond of doing), I think it is more educational to outline what [type of gear](#) is, arguably, best suited for the task

at hand. Regarding EDC, I think the following types of gear are what you might want to consider carrying on your person throughout the course of [a normal day in your life](#):

- Wallet
- Keys
- Telephone
- Watch
- Pen
- Notebook
- Fire-starter
- [Paracord](#)
- Flashlight
- Piece of cloth
- Sun protection
- [Multitool](#)
- Knife
- Firearm

As you can no doubt tell, virtually all of this equipment can be carried on your person without the need for a bag or purse (although to be fair, [some EDC practitioners use fanny packs](#)). To elucidate a bit further, sun protection would be something like a hat or sunglasses, fire-starters would include matches or a lighter, and pieces of cloth would be either a bandanna or a handkerchief. Of course, your choice of fashion might limit or expand your ability to carry, so keep that in mind, especially when choosing whether to wear pants and/or a jacket.

Grey man, as an idea, has become confused with dissimilar approaches as of late. The [vonu strategy](#) is an anti-political lifestyle of voluntary social exclusion, where it is believed that the best way to avoid being coerced is to remove yourself from all influences of coercion; “to vonu” means to disappear, presumably, by going off-grid. “[Ghosting](#)” is the act of suddenly ending a romance with absolutely no warning or a decent opportunity for closure (such as by [breaking up](#)). [Paper-tripping](#) is the practice of constructing and using alternate identification; the phrase “to go on a paper-trip” refers specifically to building such a new ID from scratch. Needless to say, paper-tripping, ghosting, and the vonu strategy are *not* the same thing as going grey, since being a grey man, much like the rest of security culture, can be easily integrated into your current lifestyle.

If most “activists” decided to go grey, they wouldn’t be activists anymore, quite frankly. Being the grey man requires a dedication to truly valuing the [right to privacy](#). All things being equal, content producers within the [alternative media](#) (like bloggers, podcasters, and videographers) usually have a sliding scale of growing public exposure the closer their medium approaches television, yet, what determines whether or not they can actually practice being a grey man is their dedication to [individual privacy](#). Although it is true that those in front of a camera are less likely to be successful grey men than those behind a keyboard, this should not serve as a source for discouragement, because with the right demeanor, just about anyone can disappear into a faceless crowd of stereotypes.

How to Make Your Car Inconspicuous

 thelastbastille.wordpress.com/2013/05/13/how-to-make-your-car-inconspicuous/

5/23/15 UPDATE: A paragraph has been added on the necessity for keeping your automobile clean in order to aid in its inconspicuousness, as well as inserted phrases and grammatical corrections throughout the original content, which has otherwise not been changed.

It is literally impossible today to avoid the government roads. The entire physical infrastructure has been built around the use of the automobile, thus increasing travel distances considerably than what they were a century ago. Once you factor in the [surveillance police state apparatus](#), then the traffic cameras and roving patrol cars suddenly take on a new importance.

As you travel from home to work and then back again during your daily commute, you are on public display for everyone to leer at. It matters not whether you have the latest in German automotive engineering under the hood, or a total lemon; what is important is what is aesthetically observable. Since quite a bit of the American population still values [conspicuous consumption](#), the more beautiful your car is, the more likely other drivers will look at you.



If you've ever noticed, those cars that have bright, shiny colors attract a whole lot more attention than the ones that possess bland, dull color schemes. [Sport utility vehicles](#) and pickup trucks that sport ostentatious accessories such as winch bumpers, fender flares, and spoilers are just begging to be profiled. Needless to say, blaring loud music with the windows rolled down, or leaving designer label shopping bags in the back seat, might just attract the kind of attention you'd prefer to not have. Just as bad though, are those hippie looking cars laced with bumper stickers advertising whatever political dogma happens to be in vogue *this week* (to be fair though, bumper stickers are still valuable as culture jamming devices [if used as adhesives with homemade posters](#), or even as identifying markers on the backs of laptop screens).

The main idea here in transforming your car into an inconspicuous one is fundamentally rooted in the principle of [the gray man](#). Just as you would dress and behave in such a way that doesn't shout "[sheepdog](#)," similarly you don't want your car to shout "wealthy target" or "anti-[Establishment](#) troublemaker" either. Your ultimate goal is to blend into the surrounding human environment; in most locales, a Ferrari will get you noticed, yet in some suburban areas, a ratty looking pickup truck with the back cab window covered in duct tape, might be even more of an eye sore. Sedans, vans, and trucks are only a few of the types of cars that usually tend to be able to blend in just about everywhere.

To further elaborate on applying the gray man principle to your car, I'd also suggest making the effort to keep your car as clean as humanly possible. Regardless of the social environment you find yourself in, being dirty is a great way to get easily noticed, much like those [off-roading](#) hobbyists who just finished their weekend [mud bogging](#). By keeping both the interior and the exterior of your car fairly clean, you

reduce the possibility of not only garnering unwanted attention, but also from serving as a collection of potential evidence that could be used against you later in a court prosecution, such as with fingerprints or DNA samples. Make sure you stow away whatever is [easily observable](#), lest you be [unjustly profiled as an undesirable](#).

Since [approximately half of all police-citizen encounters are traffic stops](#), it would behoove you to prepare for such possibilities ahead of time, preferably with the goal of avoiding them altogether. Besides [role-playing police interrogations](#) with trusted friends, you can drastically lower the probability of being pulled over if you don't call attention to yourself in the first place when you are traveling, especially if you are in the middle of [violating *mala prohibita*](#), such as by practicing [civil disobedience](#). Even when you have parked, a temptation could likely exist for the local police to seize your car using [civil asset forfeiture](#).

At the end of the day though, if you choose to adopt the gray man persona at least in the context of "driving" on the government roads, you will be taking away the excuses that both the private and government criminals have to mess with you in the first place. The defensive measures I've outlined here will increase your privacy, thus giving *you* control over what malevolent, or even nosy, strangers happen to know about you. What better way to lower their guard than by keeping them guessing?

Home Hardening: How to Fortify Your Domicile Against Intruders

www.thelastbastille.com/2016/06/22/home-hardening-fortify-domicile-intruders/

“The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail – its roof may shake – the wind may blow through it – the storm may enter – the rain may enter – but the King of England cannot enter – all his force dares not cross the threshold of the ruined tenement!”

– William Pitt

Castle doctrine has its roots traceable to the English common law, specifically the [Semayne’s Case](#), 5 Coke Rep. 91 (1604). Sir Edward Coke, the Attorney General of England, reported that:

“The house of every one in his castle, and if thieves come to a man’s house to rob or murder, and the owner or his servants kill any of the thieves in defence of himself and his house, it is no felony and he shall lose nothing.”



This is what now would be called justifiable homicide, yet the concept of using lethal force to defend one’s home, as is evidenced by this case, is about 400 years old. [Stand-your-ground laws](#) negate any [duty to retreat](#), as enumerated in [Texas Penal Code §§ 9.41 – 9.43](#); the 2007 [Joe Horn shooting](#) in Pasadena involved the direct application of castle doctrine, and thankfully, the grand jury issued **no bill** against Joe Horn for killing the two burglars.

Interestingly enough, the 1604 *Semayne* case also contained a prohibition against government for violating the castle doctrine, as well. Sir Coke reported the following:

*“In all cases where the King is party, the sheriff may break the house, either to arrest or do other execution of the King’s process, if cannot otherwise enter. But **he ought first to signify the cause of his coming, and make request to open the doors.** Where the door is open the sheriff may enter, and do execution at the suit of a subject, and so also in such case may the lord, and distrain for*

*his rent or service. **It is not lawful for the sheriff**, in request made and denial, at the suit of a common person, **to break the defendant's house**, to execute any process at the suit of a subject. The house of any one is only a privilege for himself, and does not extend to protect any person who flies to his house, or the goods of any other which are brought there, to prevent a lawful execution and to escape the process of the law: in such cases after request and denial, the sheriff may break the house. **If the sheriff might break open the door to execute civil process, yet it must be after request is made.**" [emphasis added]*

Notice that castle doctrine is not just a general prohibition against street criminals, but also a specific prohibition against "law" enforcement, which regulates them to produce a real cause to damage someone's home, and even then, they are further restrained to only commit such damage in the pursuit of a fugitive. An individual who uses force against the government's police raids is justified in doing so pursuant to [Texas Penal Code § 9.31\(c\)](#). All of this crap where the SWAT teams come in and straight up kill people's pets is not only unconscionable, but also quite indicative of the political situation Americans face, whether that manifest itself in the form of [dragnet wiretapping](#), [civil asset forfeiture](#), or [political prisoners](#), each of which is indicative of **textbook tyranny**.

Whether it be private or public criminals, the law is clearly on the side of the homeowner; the only real question left to answer is, *how does one go about hardening their home against forceful invasions?* I would suggest that the [private production of security services](#) is rather pronounced in the technology that has been invented within the home security industry. Products have been developed that serve as either add-ons to pre-existing building structures, or as renovation projects that might also improve a home's resale value.

Windows are, probably, the single most vulnerable point in any building. They can break quite easily if just enough force is used, preferably at its weakest point, which would be at the center of the pane. Obviously, the only real problem for burglars is that this creates undesirable noise, yet, if a gang has converged on a single locale for a "breaking and entering" operation, then noise might be considered a lower priority for them.

[Safety and security window film](#) is the retrofit option, given that it can be applied to pre-existing windows. [These films range in price from \\$20 – \\$50 per roll](#), depending on size and quality. The other type of product would be to invest in some type of [safety glass](#), and then have that installed as part of the building, thereby replacing the original windows. Any sort of [bulletproof glass](#) is going to range from [several hundred dollars to a few thousand dollars](#), at least. Before investing in either option, be sure to watch demonstrations of how effective these types of security windows really are; I personally recommend watching the demonstrations of [3M's window film](#) and [Innotech's security glass](#).

Next up would be the doors and entryways into the structure in question. Second only to windows in terms of vulnerability, door manufacturing really **hinges** on quality (pardon the pun!). Solid core doors are preferable, but [the norm appears to be hollow core](#), simply because they are lighter, cheaper, and easier to install than solid core.

Generally speaking, you either need to add a door brace of some kind, or replace the door itself. The [Katy Bar](#), or better yet, [the OnGARD](#), are bracing options that do entail some modification to either the door frame or the floor for installation; they cost [\\$225 – \\$325 & ~ \\$100](#), respectively. [Timber Composite Doors](#) appear to be quite resistant to leveraging and brute force, and they range in price from [£1,047 – £1,566](#) (\$1,528 – \$2,285).

Most criminals wouldn't think of barraging through walls, but some types of material can be susceptible to [sledgehammers](#) and [reciprocating saws](#), especially drywall. The only real defense I can think of would be to construct a [cinder block retaining wall that is reinforced with rebar and concrete](#). The [average cost per cinder block is approximately \\$2](#), a [Weyerhaeuser ½" by 10' rebar](#) cost about [\\$4 – \\$5](#), and an [80lb. bag of concrete mix](#) cost about [\\$4](#); from these base prices, you'd have to multiple how many cinder blocks, rebar, and cement bags you'd

need to construct a retaining wall, in regard to both its length and height. Obviously, the additional costs of water, masonry tools, and possibly sand ought to be budgeted in, as well.

Unlike [caper movies](#), most robbers are not cat burglars. I honestly wouldn't worry about your roof, unless you have a skylight, in which case the aforementioned options for windows should handle any conceivable vulnerability. Given the time and effort involved in vertical ascent, presuming that SWAT teams are going to puncture through the roof and rappel down is just plain silly; [actual police raids are much more horizontal](#).

When it comes to early warning systems, I think way too much faith has been placed in technology. Alarms and especially surveillance cameras give a false sense of security, and they can be easily defeated by "black hat" hackers, or otherwise be rendered ineffective during a black out or grid-down scenario. My recommendation is that you get a dog; [according to Hans-Hermann Hoppe](#), humanity experienced an evolutionary development in enforcing property rights when wolves became domesticated and were bred for human service.

Regarding boobytraps, it's preferable to focus on emplacing uncomfortable barriers rather than painful contraptions. For example, [Eric English said he intended to plant blackberry bushes underneath his first floor windows](#); not only would he have a source of food, but those plants would serve another purpose in deterring would-be looters. Any type of [prank](#) could be adapted for home security, especially if it were concentrated in a bottleneck within the structure's very own architecture, such as a narrow hallway or a staircase.

Should your domicile's exterior become penetrated, having a [safe room](#) would become invaluable during such an emergency. The only real problem with such a panic room is the danger of inadvertently putting yourself in a corner, but such a vulnerability can be avoided if you simply construct an escape hatch within the safe room, which is also a [design feature that is incorporated into some modern bunkers](#). As such, having an agreed upon bug out plan with your family *prior* to a home invasion of any kind is not completely unwise, especially if constructing a panic room, or otherwise converting an area into a makeshift safe room, is not possible.

Of course, if your makeshift safe room is breached, killing the intruders becomes a very real and immediate option. Once you have taken [self-defense seriously](#), then it's just a matter of choosing your weapons and employing your techniques. [Learning how to clear rooms](#), both with and without a firearm, is invaluable should you decide to take the initiative in ridding your home of violent trespassers; ideally, you should have at least one other person helping you clear your home of intruders – all these fictional portrayals of older men clearing their houses *alone* and *in the dark* is just asinine.

Understanding how to harden your home is useless without also comprehending the strategic thinking used to implement it. Apartments are more difficult to harden than houses, and even then, you could become gypped on hardening *rented* houses if you decide to renovate the structure, and then you decide to move out not long afterwards; therefore, structural changes to windows, doors, and especially walls are really only beneficial to a homeowner. The idea here is to have a multi-layered defensive structure not unlike the layers of an onion, hence the exterior defenses of the windows, doors, and walls followed by the interior defenses of the boobytraps, safe rooms, and (presumably) firearms.

If you did a good enough job hardening your home, then during an emergency (whether that be a burglary or a police raid), you shouldn't have to kill anybody. It's important to emphasize that you should *never* let fear rule your life; so, take some time and *calmly* think through what your options realistically are, **what your budget allows**, and *act* accordingly. Privatizing security begins with *you*, the customer, providing a [market demand](#) for goods and services by beginning to take precautions with the intention of making yourself [less vulnerable to coercion](#) that potential adversaries might try to impose upon you.

Interpersonal Diplomacy: The Value of Keeping the Peace

 www.thelastbastille.com/2012/11/26/interpersonal-diplomacy-the-value-of-keeping-the-peace/

2/24/16 UPDATE: In learning more about [diplomacy](#) and [etiquette](#), I realized this article really needed a serious overhaul. Entire paragraphs have been deleted and brand new ones added, with only a few elements kept from the original version. I sincerely hope this revision is more helpful to you all.

"I often used to find myself in conversations with people who are self-destructive and negative. They were so ardent when describing their negative self-image to me that my protective, nurturing instincts kicked in and I would find myself trying to massage their ego, in some misguided attempt to bolster their confidence and shake them out of their pessimistic view. I invariably failed; my belief in them and their potential was clearly never as strong as their own belief that they were ugly, shy, unable, or whatever it might be. They were completely enraptured and hypnotized by the little voice in the back of their heads, the one who pretends to be your friend but secretly wishes to destroy your entire life...the trouble was that once I was sold on their idea of themselves, I was no longer as interested in their company because I invariably felt completely drained afterward. Eventually, I developed a new tactic, a new response for dealing with their self-loathing, one that never fails. 'If you say so.'...You've just managed to reach the place thousands of mystics and seers have struggled to attain through years of meditation, and all with four little words. And without Prozac. My gift to you. You're welcome."

– [The Anti-Terrorist](#)

Diplomacy, [simply defined](#), is a "skill in dealing with others without causing bad feelings." Given that [only individuals exist](#), whatever cooperation is available in this world is made possible not by "society," but by individual humans. Therefore, the utility of etiquette is to function as a "social lubricant," especially in the context of superficial interactions between two people who would otherwise not naturally get along.

A large part of the reason for adages such as, "In polite society, don't talk about politics, sex, or religion," is to grease the skids of business negotiations, as well as other tense scenarios where the window of time you spend with particular strangers is already quite small.

Whether it be [police interrogations](#) or Thanksgiving dinner with extended family, refraining from talking about divisive topics with *some* individuals might just keep the peace. Techniques such as "[non-violent communication](#)" (NVC) have the potential to smooth over tensions, yet the experience of being the [grey man](#) during a [political fieldtrip](#) shows that discretion really is the better part of valor; simply put, while you could invest time and money into learning NVC, you could just lower your opportunity costs by avoiding fruitless "[debate](#)" with disagreeable individuals.

Good [role-modeling](#) is vital whenever one is attempting to use diplomatic tact. Two months ago, [I got accused by James Babb of "issuing orders" to the audience](#) for merely suggesting other approaches to teaching folks about [jury nullification](#) (as well as the method of jury nullification itself). I only mention it here to illustrate how the sheer lack of basic etiquette can really turn people off to anything else you may have to say, and even statisticians complain about this phenomenon. If an indispensable element of securing our liberties is "winning hearts & minds," then I fail to see how inconsiderate manners in the public arena furthers the accomplishment of that goal.



[Internal balkanization](#), which is colloquially known as “infighting,” often happens when there is a lack of interpersonal diplomacy. Such occurrences could have been avoided if at least one of the parties, if not preferably both, had acted like adults with the simplest of etiquette. Failure to [keep your own counsel](#) is an excellent way to burn bridges with business associates, open-source intelligence contacts, and even political alliances. All you have to do is peruse the examples of miscreants like [Jim Stach](#), [Rick Light](#), [Jerry DeLemus](#), and [Brandon Curtiss](#) in order to understand that not adhering to the biblical golden rule of “treating others as you would like to be treated,” only sets the stage for counter-productive bickering and demoralization.

[Peaceful coexistence](#) with a variety of individual personality temperaments is the whole point of “killing them with kindness.” Learning social graces is an admirable pursuit, but don’t allow it to overwhelm your own sense of self; you’re an individual, too! Practiced empathy is what you’re aiming for, and this comes from quiet confidence, *not* insecure psychobabble. [As Thomas Jefferson said in 1785](#):

“The legitimate powers of government extend to such acts only as are injurious to others. But it does me no injury for my neighbour to say there are twenty gods, or no god. It neither picks my pocket nor breaks my leg.”

Keeping the peace is a balancing act, and I only care about what others (might) think about me to the extent it affects my own freedom; otherwise, they’re entitled to their own opinion, which, just like assholes, everyone has one, so it’s no skin off my nose.

Disingenuous Activists! Why Leaderless Resistance is Preferable to Formal Organizations

□ www.thelastbastille.com/2016/04/14/disingenuous-activists-leaderless-resistance-preferable-formal-organizations/

“Avoid membership in political groups or other civic organizations. As a rule, these groups are filled with super sneaky, nosy individuals more willing that not to stab someone in the back if it suits their selfish purposes. Total snakes.”

– Barry Reid

People ought to collaborate whenever they can in order to achieve their goals. Individuals who become familiar with each other have the potential to develop a [molecular level bond of trust](#), which is essential for the smooth operation of any activities they may choose to perform. However, joining a formally organized activist group, much like using [“suspicious” email keywords](#) or [custom aluminum warning signage](#), is usually more trouble than it’s worth.



[Populism](#) is usually the driving force behind activists who feel the need to organize, whether it be nationally or in their local communities. This [democratic impulse](#) is typically based on the assumption that the [theory of critical mass](#) is valid, despite all historical evidence that suggests foundational change is normally caused by relatively few people, as is the case, for example, with a [coup d’état](#). The reason [socio–political movements](#) rarely achieve their stated goals is, more often than not, due to the simple fact that with the greater adoption of their professed values, their principles become diluted as the sheer number of self-identified adherents grow – this is source behind the derisive phrase, “cultural bowel movement.”

Truth be told, populism is really just another form of [collectivism](#). Whether the specific context is nationalism or egalitarianism, the operating presumption is that “we” are all in “this” together, whatever that may be. All too often, [reformism](#) becomes the *modus operandi*, thereby leading its practitioners down the road to perdition; [as Larken Rose has said](#):

“Most ‘activism’ is completely worthless; in fact, it’s worst than completely worthless [because] it accomplishes more harm than good...I speak from experience. Many, many years ago, when I still believed in statism, I was politically active, and I campaigned, and I played those games, and I wrote my congressman, and did all that stuff (I’m kinda embarrassed to admit it now), but, yeah, I did that

*too. At the time, I really and truly believed that I was ‘fighting the right fight,’ [that] I was fighting against the beast. It only occurred to me many years later that I was actually **feeding** the beast lots and lots of fuel.”*

This rather profound insight shows the gaping hollowness permeating formally organized activist groups. How can reflexively spouting that **education is the answer** to every single problem be true if such “education” is rampantly littered with **misinformation and disinformation**?

If **political fieldtrips** are to serve any useful function, it is that the exercise of this technique will break the back of populism’s legitimacy within the minds of its victims. Once you personally witness Leviathan, under normal circumstances, acting within its own natural habitat, the sheer horror that is the daily routine of government will also become equally apparent in the **politicking** that is all too common within “organized” activist groups, as well. In short, formal activist organizations are a reflection of **the State** itself, especially considering their top-down organizational structure with regional chapters who report back to their centralized headquarters.

Whether it be labeled the patriot, liberty, or truth “movement,” those individuals who demand more freedom usually attempt to organize themselves in the hope that doing so will serve as a **force multiplier**. Presuming this were true, then what could possibly explain when the polar opposite, as a matter of course, becomes the typical result? The history of contemporary activist organizing suggests to me that ulterior motives, especially when coupled with a naïve misunderstanding about **how** an organization seeks to achieve its stated goals, creates an atmosphere of disingenuous rhetoric and moral hypocrisy.

Consider, for a moment, when the **Constitutional Sheriffs and Peace Officers Association** (CSPOA) publicly issued those **letters written by county sheriffs** who voiced their opposition to the federal government’s proposed unconstitutional gun control measures, back in 2013. Similarly, was the **Tenth Amendment Center** (TAC) successful in nullifying unconstitutional federal actions vis-à-vis the passage of **HB 910** right here in Texas last June? Are the Three Percenters truly going to protect America on the off-chance that the **Schumer hits the proverbial fan**? I’d suggest that CSPOA’s released letters simply reinforced a misunderstanding about the viability of “**constitutional sheriffs**” in securing the right to keep and bear arms, that HB 910 had nothing whatsoever to do with TAC’s advocacy of state “**nullification**,” and that the **Idaho Three Percenters** will flee at the slightest sign of real danger, as they did last February when **they abandoned the Final Four at the Malheur refuge into the waiting jaws of the FBI**.

In 2009, Luke Rudkowski solicited donations intended for a legal defense fund on behalf of himself and two other members of *We Are Change* to the tune of **\$4,241.55** that still remains unaccounted for, in clear violation of the WAC Code of Conduct. During 2013, Adam Kokesh’s employees never accounted for the check that George Donnelly sent *Adam v. The Man* for **\$5,431.58** – despite that they never disputed the fact that Donnelly had already sent AvTM 4.5002619 Bitcoins & 120.5 Litecoins (~ \$450 & \$284, respectively). Speaking of Bitcoin, Coin Center and the Bitcoin Foundation are quite fond of “**building relationships**” with federal regulators who desire to centrally plan every facet of life from cradle to grave; **when I attempted to warn Bitcoiners about this last year**, few of them seemed to give a damn – the lack of righteous indignation truly does mean, at least to my mind, that **the silence is deafening** (**no wonder Bitcoin developer Mike Hearn quit!**).

Also in 2013, **Christopher Cantwell was formally ostracized from the Free State Project** (FSP) by its Board of Trustees for reminding everyone of their common right of revolution, which is enumerated in **Article 10 of New Hampshire’s Bill of Rights**. Later that year it was revealed that none other than Free Keene’s **Ian Bernard was the individual who encouraged the FSP Board to scrutinize the rhetoric of Larken Rose**, as if **ritualistic purges** are necessary in order to rid “**the Party**” of assorted undesirables. Not only did **Cantwell and Bernard have their own falling out** last year, but **once the FSP reached its “goal” of 20,000 signers** to the non-contract that is the Statement of Intent earlier this year, they were all too quick to **formally ostracize Bernard himself**, oh-so-conveniently **a mere**

three days before [the FBI raided Bernard's home in Keene](#).

Why anyone would bother paying for tickets in order to attend [Liberty Forum](#) or the Porcupine Freedom Festival (aka, "[Porcfest](#)"), or otherwise continue donating money to the FSP, in light of their treatment of **both** Cantwell and Bernard, is truly beyond me. Even Bernard, of all people, didn't deserve that kind of treatment, given that in *this* country, there is such a thing as the presumption of innocence until *proven* guilty. Yes, it is true that I have advocated for a [boycott of Free Talk Live](#) for two years now (and still do), but how Bernard was demonized here is beyond appalling, especially considering it is a well-known fact that Bernard was the FSP's most successful recruiter; once the FSP Board had achieved their fake goal, they were all too quick to cast him out into the cold alone to be at the mercy of the government's wolves, weren't they?

During the [Bundy Affair of 2014](#), the Oathkeepers attempted to pick a fight with the various militia units, many of whom responded to a call out by Operation Mutual Aid (now known as [Operation Mutual Defense](#)). When the fake drone strike occurred, the Oathkeepers fled and left the women and children at the Bundy Ranch to suffer what thankfully never transpired, yet in the aftermath of the 2015 Chattanooga shootings, [Operation Protect the Protectors](#) was launched in order to have people stand guard at the military recruitment stations (despite the evils committed by the [warfare state](#)). This is why they are now derisively referred to as the Oathbreakers, not to say how they also conveniently abandoned [Charles Dyer, who was their U.S. Marine liaison](#).

Between 2014 – 2015, the [absorption and dilution](#) of the [Jews for the Preservation of Firearms Ownership](#) (JPFO) by the [Second Amendment Foundation](#) (SAF) was outright scandalous. Alan Gottlieb disgraced Aaron Zelman's legacy thoroughly, so it is no exaggeration to say that the JPFO sellouts on the board of trustees offered their organization up on a platter to the SAF, without so much as consulting their membership at all. The transferral of the rank-and-file membership's [personally identifiable information](#) from JPFO's mail lists to the SAF, **without** their consent, is a grave breach of security culture, to say the least.

Similarly in terms of violating privacy, [Mark Kessler's III% Boots on Ground and Constitutional Security Force](#) tricked some American patriots into filling out an rather invasive [application for membership](#). As Gary Hunt described it:

"Nearly every person who joined the III% BOG completed and sent to Kessler an application, sufficient in detail to positively hundreds, perhaps thousands, who joined his organization. The information requested is far more extensive than you would fill out for a job, and includes questions that are appropriate for psychological evaluation, or profiling."

When Kessler outed himself as a government informant on the December 2nd, 2014 broadcast of [The Alan Colmes Show](#), this confirmed he was serving as a (non-sexual) [honeypot](#), of sorts. According to Hunt's partial transcription of that interview, Kessler admitted the following:

COLMES: How many people would you say came out of the woodwork, or how many groups came to you as a result of the bait that you threw out there?

*KESSLER: Thousands and thousands and thousands; **they have no idea**...*

COLMES: And what? You turned them over to the feds?

KESSLER: My job was to find out if they were dangerous or not. If they were a dangerous group or deemed a threat to society, well then, **we took care of business**.

* * *

COLMES: How is your name not attached to this? You don't want to tell us what agencies, where you got this information, who you work for?

KESSLER: I was intel, I was strictly intelligence.

* * *

COLMES: Where can the citizens go and see the results of this? Is there any place we can learn more about it?

KESSLER: My part is finished. I'm not at liberty, I can't reveal which agencies...

COLMES: Will there be a time when you will be able to reveal that?

KESSLER: Yes, I'm sure there will be, but right now, there are still pending investigations going on. I cannot reveal what's going on...

Notice that Kessler admitted he had engaged in [unjust profiling](#), on the thinly veiled excuse that such targeted individuals were "deemed a threat to society." So, if you were to put together the invasive questions on the III% B.O.G membership application (which is rife with misspellings) with Kessler's very public confession, I think it is more than safe to say that Kessler was quite disingenuous toward those individuals who consider themselves patriotic militiamen.

Not that joining a formally organized activist group is a one-way ticket to a government dungeon by any means, for it is also equally possible that they will lead you by the nose through sucking time and money away from you **with** your consent, simply because you believed in their pabulum. [Texans for Accountable Government](#) (TAG) has really gone downhill in recent years, yet, I remember when [John Bush](#) really worked that group as its executive director. Although the charismatic [Katie Brewer](#) and the wonderfully firebrand [Heather Fazio](#) were still there as of last year, I doubt even they can "rescue" it from [Justin Arman](#) and his reformist allies like [Dr. Laura Pressley](#), nor should they.

Off-grid homesteaders are not immune from the corrupting influence of other activist organizations, for the fate of the [SLV Just Us](#) group in Costilla County, Colorado last year testifies such to be the case. They were able to withstand the pressure from both the Costilla County government and the bigoted Hispanics within the Town of San Luis, but when [Operation Patriot Rally Point](#) rolled on in, the homesteaders were balkanized so badly they were unable to recover. [As Alex Ansary commented](#) three days after the disastrous "Meet the Judge" event:

*"I will **never** trust certain people to vet certain people **ever** from this point on. It is **irresponsible** to assume other people will just do the vetting for us and vet certain members, and make sure they are who they say they are; well, that wasn't done. **No group or community can be fully safe if people are so naïve that they don't even bother to question, or look up, the supposed people that are coming to the rescue.**" [emphasis added]*

This rather harsh truth illustrates the fact that when activist organizations clash, the fall-out is bound to be a degradation of solidarity, not a reaffirmation of it. Just because people have grievances and are seeking remedies to alleviate them, does not therefore mean that such proposed techniques are effective at remedying those grievances. When there is a difference between activists regarding strategy and tactics, it is a *fait accompli* that the sparks will fly, thereby leading to schisms and overall fracturing, unless [interpersonal diplomacy](#) takes place quickly in order to mitigate friction.

Sometimes the breakdown will not occur as a flashpoint, but rather, as a slow deterioration. The [Williamson County “Libertarian” Party](#) (WCLP) never had the membership who attended its meetings like TAG did, and it carried along with it the additional baggage of not only [partyarchy](#), but also [the confession made by the national LP founder David Nolan in 2008](#) about the monster he had created:

*“We have, unfortunately, created (or the party has created) a little class of mini-bureaucrats who are more concerned with keeping their job and perpetuating the institution as an institution and raising money, than they are with spreading the message...now we’re down to the level of people who are, I think, for the most part, well-intended, but when compared to those men [i.e. Murray Rothbard], are several orders down the intellectual scale, and they’re absorbed with minutiae, and they are concerned with fund-raising, and they are afraid to say anything that might scare people, because that might keep people from voting for us, so it’s become a very **timid** organization in the last 6 or 8 years.”*

When you additionally consider that the WCLP’s own Robert Butler brazenly took credit for something neither he nor the WCLP did last year regarding a few red light traffic cameras, then the disingenuousness the anti-libertarian “Libertarian” Party oozes forth becomes rather apparent, as was also the case with Shane Radliff’s political fieldtrip to a meeting of the [McLean County “Libertarian” Party](#) (MCLP) last year.

The latest of these organizational travesties is the bickering amongst [“sovereign” citizen](#) groups, most notably the “Continental uNited States of America” and the National Liberty Alliance. [As you may remember](#), the latest “sovereign” citizen trend has been for some of them to become fake judges and then convince others that they are the same as the flowing black-robed men. Bruce Doucette, specifically, balkanized the SLV Just Us group, as well as inserting himself into the [statist turf war](#) not too long afterwards.

Assuming that the rule is that formal activist organizations are not conducive to your freedom or privacy, then what would be the exception to that rule, if any? Organizations such as the [Home School Legal Defense Association](#) (HSLDA), the [Texas Home School Coalition](#) (THSC), the [Institute for Justice](#) (IJ), the [Foundation for Economic Education](#) (FEE), the [Ludwig von Mises Institute](#) (LvMI), and the [International Society for Individual Liberty](#) (ISIL) seem to have a few traits in common. Either these are purely educational, as is the case with FEE, LvMI, and ISIL, or they are engaged in some form of legal activity, like what THSC, HSLDA, and IJ do.

Of course, when evaluating the purported accomplishments of any formally organized activist groups, it might become useful to compare them to those similar activities by individuals whose efforts are directly parallel. The [New Hampshire Liberty Alliance](#) (NHLA) has produced Liberty Rating reports for twelve years now about the [New Hampshire General Court](#), yet, I would suggest that Chris Cantwell’s [Anarcho-Lobbyist](#) series is noticeably more transparent, and without all of the overhead. Although the FSP imagines itself as having “accomplished” 20,000

signers, it would seem to be the case that people are flocking in droves into the American Redoubt, as well as the American West more generally; the best transparency for this comes from [John Schmidt](#) and [Alex Ansary](#), respectively.

Most importantly, the violations to security culture posed by activist organizations is staggering. Whether it be due to [snitches](#), [datamining](#), [snitch-jacketing](#), [doxxing](#), [false accusations of stealing from legal defense funds](#), or potentially even [losing your job](#), joining most activist organizations will likely increase your opportunity costs at the very least, and reducing your freedom at worst. In other words, all things being equal, it is more than fair to say that activist organizations are more trouble than they are worth.

[Leaderless resistance](#) is the best alternative to formal organizations, from what I know. Briefly, leaderless resistance enjoys the traits of [affinity consensus](#), [mutual aid](#), and [plausible deniability](#); in other words, **simplicity**, **flexibility**, and **privacy**. Applications of leaderless resistance include [security teams](#), [freedom cells](#), and even the alternative media itself.

[As I've mentioned in the past](#), everything I've done to free myself has been done either alone, or in concert with other individuals through fluid peer-to-peer relationships. Formally "organized" groups are much too top heavy in practice, and in fact, impose drastic opportunity costs upon their memberships. By contrast, leaderless resistance is, I think, the best approach to "organizing" libertarians and other individuals, whether the purpose for doing so is a business cooperative or [monkey-wrenching](#). Top-down, hierarchical "groups" get infiltrated, whereas interpersonal relationships are really only susceptible to blackmail and extortion, at most; this makes them noticeably harder to penetrate and disrupt.

Organizations don't matter, **but** relationships do. Formal activist organizations, when all is said and done, end up **destroying** any semblance of solidarity. Celebrity gatekeepers effectively neutralize grassroots "movements" for the benefit of the enemy, and in this respect, those "[celebritarians](#)" and [Patriot Rockstars](#) are little different from the [Volksdeutchers](#) in Nazi-occupied Poland. The only real purpose for these formally organized "groups" and "movements" is not to accomplish their stated objectives, but rather to provide [an advertising brand that its membership will self-identify with](#) (and donate money to), by feeling good about doing nothing productive at all.

Activist organizations are highly overrated in their efficacy for securing individual liberty. Too many of them are organized like a pyramid, and if Americans are going to enjoy liberty within their lifetime, then that pyramid **must** be flipped upside down. Truly grassroots "organizing" means doing so from the bottom-up. Whether organizing models like the emerging *local* [Committees of Safety](#) (or libertarian grassroots entities such as [Liberate RVA](#) and the [Houston Free Thinkers](#)) are worth anything in this modern age, remains to be seen, yet, it is my hope that upon further investigation, these different ways of coordinating human action, as the purposeful behavior that it is, will yield an answer.

You Are Known By the Company You Keep: How to Choose Your Allies Wisely

www.thelastbastille.com/2016/02/25/you-are-known-by-the-company-you-keep-how-to-choose-your-allies-wisely/

“Associate yourself with skilled doers, not ‘talkers.’ Seek out people that share your outlook and morality. Living in close confines with other families is sure to cause friction but that will be minimized if you share a common religion and norms of behavior. You can’t learn every skill yourself. Assemble a team that includes members with medical knowledge, tactical skills, electronics experience, and traditional practical skills.”

— James Wesley, Rawles



Free association is an application of the libertarian principle that is the **self-ownership axiom**, namely, that **individual humans** enjoy absolute property rights in their own person, and as such, they are free to choose whom they will associate with voluntarily; conversely, this also implies the **right to disassociate**. Similarly, the **freedom of contract** is a parallel application of self-ownership as well, and as such, the right to refuse service, much like the right to disassociate, is another voluntary way to **keep the peace**. This freedom of association is implied by the **freedom of assembly**, which is constitutionally recognized by the **United States Constitution's Free Assembly Clause** within the First Amendment and the Texas Constitution's **Art. I §§ 27 & 29**, which say, respectively, that:

“Congress shall make no law...abridging...the right of the people peaceably to assemble...”

“The citizens shall have the right, in a peaceable manner, to assemble together for their common good...”

“To guard against transgressions of the high powers herein delegated, we declare that everything in this ‘Bill of Rights’ is excepted out of the general powers of government, and shall forever remain inviolate, and all laws contrary thereto, or to the following provisions, shall be void.”

Despite these constitutional clauses, both the federal and Texan governments [unjustly profile Americans in order to chill their dissent](#). For this reason, American citizens will be able to freely associate once they begin using [security culture](#) techniques.

Failure to abide by security culture increases the likelihood of becoming a [political prisoner](#). William Wolf was arrested for violating Title 18 United States Code § 922(o) for “possession” of a “machinegun” that was, in actuality, a shotgun; this was only possible because Ed Gray was acting as a [confidential informant](#) for the [Federal Bureau of Investigation](#) (FBI). Similarly, Schuyler Barbeau was arrested for violating 26 USC §§ 581(d) & 5845(a)(3) for “possession” of an unregistered “firearm” whose rifle barrel was less than 16 inches long; this was only possible because Oliver Murphy was acting as a confidential informant for the FBI. The only reason Wolf and Barbeau became political prisoners for committing these [victimless crimes](#) was because Gray and Murphy [snitched](#) to their FBI handlers.

Obviously, both Wolf and Barbeau had terrible security culture, otherwise they wouldn't have been informed on by Gray and Murphy, respectively. Putting aside the joys of informant hunting (by which I mean **public exposure** as such), the quite serious threat of [informants, provocateurs, and operatives](#) could seriously alter the very enjoyment of your freedom, so they are not something to be trifled with or carelessly dismissed. Regardless of geographical proximity, whether it is the local neighbors or your [Facebook “friends,”](#) the dangers of bad character might just incentivize those already in your life to emulate the behavior of Gray and Murphy, with or without financial compensation from the [government police](#).

For these reasons, it is imperative for Americans to choose their associates wisely. This necessarily entails the judicious and discretionary use of both [vetting](#) and [ostracism](#). As you would expect, vetting is the prevention whereas ostracism is the cure. Simply put, the better the vetting, the less necessary ostracism becomes for dealing with undesirable people.

Why bother seeking out associates and potential comrades in the first place, though, especially given all this hassle? The value of peer-to-peer relationships is grossly underestimated, not just in terms of their [marginal utility](#), but also with respect to the ability of [individuals](#) to complement each other, whether it be platonic or romantic in nature. Although I am an individualist, that doesn't therefore mean I am 100% self-sufficient, or would even want to be; the free market is entirely composed of individuals who **rely on each other** to voluntarily exchange their skills, goods, and ideas in mutually beneficial trades. To that end, individuals must learn how to “size each other up,” and the [spontaneous order](#) of a business' reputation for being trustworthy and “keeping private matters private” is an illustrative example for how vetting and ostracism are expressions of market dynamics.

Where do you find people locally? In order to vet someone, you must begin looking for them, and attending political meetings is a good first step. Whether it be scheduled through a [Meetup](#) “group” or Fascistbook “event,” going on [political fieldtrips](#) is an excellent way to “get a lay of the land,” besides an opportunity to practice using a [inconspicuous car](#), being the [grey man](#), and [keeping your own counsel](#). You could also meet people one-on-one through casual encounters at outdoor supply and gun shops, or more purposively by arranging for “meet ‘n greets” with people you came across on a discussion forum board, email list, or even a NING website.

These are not idle suggestions, for I think that for someone to “talk the talk,” he ought to also “walk the walk.” My experiences last year with [Johnnie Russell](#), [Robert the Eagle Scout](#), [Katie Brewer](#), [Heather Fazio](#), [Justin Arman](#), [Robert Butler](#), and [Bo Zimmerman](#) amply demonstrate that I practice what I preach. Although I have no interest in publicly disclosing the best examples of vetting and ostracism in my encounters from years past with a variety of survivalist and anarchist groups and individuals, I hope that what guidance I have to offer here will be given some due credence. What I know about vetting and ostracism is based upon *practical* experience, even though these methods are validly rooted in libertarian theory.

Usually, in the course of events, people become soldiers, and then later *some* of them become spies. Analogously, “we” must learn how to be spies first before learning how to become soldiers. Guys join a militia unit expecting to

“play war,” and then they either become [embroiled in infighting](#) or fall into serious trouble with the government, so they end up finding themselves “playing spy,” “playing publicist,” or “playing lawyer,” instead. Briefly put, the skill set you must cultivate in order to attract other individuals to you is *not* the same skill set that you would use to develop your capabilities in waging [serious self-defense](#).

So, how do you choose the location and time for a meet ‘n greet? It is best to avoid heavy traffic by seeking a calm atmosphere, since presumably both of you will be acting as grey men. Taking this as a given, then it would be prudent to schedule a get-together on the weekdays *during* normal business hours (preferably, during normal [government school](#) hours as well) in public spaces, such as coffeehouses, diners, or sushi bars. Mutually agreed upon recognition symbols ought to be arranged ahead of time if you haven’t communicated by webcam or otherwise don’t know what either of you look like. In a pinch, a telephone or even VoIP call is an expedient compromise, but as alternatives to face-to-face meetings, they sacrifice body language and facial expressions, which make vetting that much more difficult to conduct well.

During the meeting, feel each other out by using your [conversational skills](#). Try to determine his likes and dislikes, his virtues and vices, his enlightened sensibilities as well as his bigoted prejudices. Remember, he should be talking at least half, if not most, of the time; vetting requires as many details as possible from a potential ally, not a lengthy sermon from a rather drab proselytizer.

[Don’t fruitless “debate” him](#). Ask him to clarify anything you might not understand, but don’t ever persist in arguing. Nothing is to be gained and everything could be lost by pushing him towards accepting your views. It is better to cultivate an ally who is 25% on your side than alienate someone to the point where he chooses to give you the cold shoulder, or worse, decides to work 100% for your enemies.

You want to give off the impression of being unassuming. Keep your body language casual yet not flirtatious. What you are essentially doing is conducting the equivalent of a job interview without it feeling like one. The idea here is to elicit information about him while maintaining the aura of a leisurely conversation. Hunching over, needlessly whispering, and otherwise acting standoffish is to be avoided. You want your prospective associate to feel relaxed yet focused on the conversation without seemingly doing so.

Once the meeting is nearly done, keep him on the hook for the time being by arranging for a *tentative* follow-up meeting. This is to give the impression that you are still interested in him without actually making a decision on the spot; you do that *afterwards* in terms of whether to “recruit” him or cut him loose. For those who are worthy, recurring face-to-face meetings ought to have a scheduled rendezvous point *different from* the actual location of the get-together, which necessitates travel between the two locales.

Vetted individuals that you have successfully “recruited” are far more likely to respect the practice of security culture, and therefore render the necessity for ostracism to be less than if they hadn’t been vetted. To reiterate, good security culture relies more heavily on vetting than on ostracism, although both are indispensably vital for choosing your allies wisely.

Speaking of which, ostracism is more complex than just giving someone the proverbial “cold-shoulder.” Shunning is *not* the same as “deFOOing,” with the difference being that the former is disassociating from one or a few individuals, whereas the latter is disassociating from your entire [family of origin](#) (this is the “FOO” in “deFOO”). Having done both, trust me when I say that shunning is infinitely preferable to deFOOing for reasons that bear further scrutiny at a later time. Suffice it say for now, “simply” shunning someone does not carry anywhere near the emotional toll that escaping both your nuclear and extended family wholesale does, due primarily to the costs of “disentangling.”

The joys of informant hunting are but one form of ostracism, yet it is quite possible that your experience in using it will be against someone far less sinister. Far more likely a candidate for ostracism is an acquaintance who fails to pass the “smell test.” One such variant of this is the litmus test that is the [Against Me argument](#), which simply asks

whether the individual being asked supports the use of initiatory force against you for simply disagreeing with him. Asking someone whether they support the use of **coercion** against you, by *personalizing* the violence inherent in the system, forces him to directly address his attitude towards you, specifically. Naturally, if they do support you being shot for simply disagreeing with them, then perhaps those individuals do not have your best interest at heart, to put it mildly.

Generally speaking, authoritarians **do** support the initiation of the use of force against you for disagreeing with them, or the government. Conversely, libertarians do **not** support initiatory violence being used against anyone for simply disagreeing, even if they take personal issue with the nature of that specific disagreement. The only question you have to ask yourself, regarding this form of ostracism, is, **do you want to be surrounded by people who want you shot?** Unlike naïve approaches to exercising your freedom, [practical politics](#) focuses on what you *can* control in your own life, rather than frittering away your precious time and effort on ineffective, or even counter-productive, actions.

Believe it or not, good [role-modeling](#) is uniquely precious, since most people I have encountered will not value [integrity over friendship](#). They do this because they are still collectivistic – they want to be “accepted” because they bow before peer pressure, they want to follow the herd, and they desire the comfort of shallow praise. Encryption of any kind does not matter if the human at the other end of the line is a person of ill-repute; consider, for example, the actions of [Luke Rudkowski](#), [Jeffrey Phillips](#), [Nancy Genovese](#), [Ed Snook](#), [George Hemminger](#), [Ron Paul](#), [Mark Dice](#), [Stewart Rhodes](#), [Christopher Blystone](#), and [Mark Kessler](#). I would submit to you that these are the types of miscreants who deserve ostracism for what they’ve done, especially because of the people most of them have scammed.

Back in 2002, [Barry Reid](#) suggested using a coded address book for all of your contacts. He said:

“Protect the names, addresses and telephone numbers of your friends. Use a code of your own making to disguise the actual names and numbers, or try to memorize what you need to know. You’d be amazed at how much you can remember in this area if you make the effort.

“Try to avoid carrying this coded address book with you. Cops always flash on such items, and so-called ‘rings’ are usually busted this way. A smart thing to do would be to carry a dummy book of names and numbers selected at random from the phone book. Keep your working book stashes in a safe place.

“This practice protects you, too, inasmuch as suspicion is cast on you should some of your friends be busted and their names appear in your book.”

Of course, nowadays it might be more practical to do so using a digitally encrypted smartphone, but it would be prudent to determine the efficacy of that at a later time. For now, just understand that once you’ve successfully “recruited” people to be your allies, *how* you go about storing their contact information is a security culture issue all by itself.

If you’ve learned nothing else from this cursory guide on finding allies and keeping foes at arms length, then I hope you would take away from all this the importance of keeping a relatively small social circle, at the very least. I know that the Fascistbook phenomenon encourages you to maintain and grow your ceaselessly expanding list of *thousands* of “friends,” but I would encourage your to aim for **quality**, not quantity. Should empty “popularity” be

important to you, then just consider the fates of political prisoners who are currently rotting away in government dungeons because too many of them failed to use good security culture in vetting and ostracizing the people in their own lives, as needed. There is nothing wrong with [compartamentalizing](#) information on a “need-to-know” basis, or exercising caution with those who turn out to be [false friends](#). Finally, ponder over this one of Aesop’s fables entitled, [The Ass and His Purchaser](#):

“A man who wanted to buy an Ass went to market, and, coming across a likely-looking beast, arranged with the owner that he should be allowed to take him home on trial to see what he was like. When he reached home, he put him into his stable along with the other asses. The newcomer took a look around, and immediately went and chose a place next to the laziest and greediest beast in the stable. When the master saw this, he put a halt on him at once, and led him off to be handed back to his owner again. The latter was a good deal surprised to seem him back so soon, and said, ‘Why, do you mean to say you have tested him already?’ ‘I don’t want to put him through any more tests,’ replied the other, ‘I could see what sort of beast he is from the companion he chose for himself.’ Thus arose the adage, ‘A man is known by the company he keeps.’”

May You Live in Interesting Times...

 thelastbastille.wordpress.com/2013/02/13/may-you-live-in-interesting-times/

In order to succeed in any worthwhile effort, people need to be able to work with each other reliably. If this is systematically disrupted by [controlled opposition](#) (or more than likely, just your run-of-the-mill useful idiot), it then breeds a culture of fear where everyone is automatically suspicious of everyone else. A certain minimal amount of trust is necessary for there to be some feeling of comraderie.



Well over a year ago, I was one of the very few individuals who blew the whistle on the prevalence of infighting within the Patriot Community; I even went so far as to coin the term, “[internal balkanization](#),” stating also that it was the #1 threat to American patriots, as well as being the chief reason why they can’t seem to accomplish much of anything positive (in the [collective aggregate](#)). Besides the lack of concrete milestones by which to measure any progress in securing our Liberties, it is also very true what [Randy Mack](#) has said time and time again – as he puts it, “[We cannot learn to work together](#).” Unfortunately, such is still the case today as I write this; both Randy and I (not to neglect the handful of others who also know better) have been proven correct (exceptions to the rule notwithstanding).

Thankfully, all is not lost. Ever since the advent of the [Committee of Safety – Common Law Court](#) (CoS-CLC), there has been a steady (albeit painfully slow) effort to “clean house” of all the [narcissistic demagogues, sycophantic cowards, and assorted miscreants](#). The only organization amongst the many political dissident circles to take the problem seriously, the CoS-CLC has provided a way to exercise the right of trial by jury outside the confines of the enemy rebel government. Without succumbing to the

horrendous practice of “trial by press,” the CLC’s Grand Juries have been able to fairly judge the accusations brought before them, with the corresponding evidence, by reaching a determination. How many other groups (of one flavor or another) can claim such a level of teamwork that produces, at the end of the day, such a result?

So, what has the CLC discovered? Oh, quite a bit, I assure you. Let’s begin with [Mascarenas v. Stachowiak](#), Verdict #110401, where wannabe “resistance leader” **James Stachowiak** (alias **Jim Stach**) was found guilty by the Grand Jury on 4 counts of defamation, 3 counts of slander, 2 counts of incitement, and 1 count of threat against **Randy Mack**. It would seem to be the case here that “**Freedom Fighter**” has no concept of [interpersonal diplomacy](#) and certainly does not [keep his own counsel](#), considering that he was more than willing to throw Randy (whom you would assume he would have thought of as a fellow brother-in-arms, even if only in spirit) under the bus without hesitation; might it even suggest where his loyalties truly lie?

Debra Swan brought charges against [WRAM](#) founder and chief administrator **Rick Light** (alias **Minuteman**) in [Swan v. Light](#), Unanswered Indictment #120201, whom was found, **under probable cause**, to have committed 3 counts of libel, 2 counts of defamation, 1 count of threat, 1 count of entrapment, 1 count of extortion, 1 count of being inimical to the Patriot Community itself, and my personal favorite, 1 count of intimidating the CLC Grand Jury. I mean, who does this schmuck think he is? That he can just get away with lying about false death threats, knowingly give a child an “illegal” firearm, and threaten to beat up a woman who has *caused him no harm*?! Actions such as these are evocative of Mafiosi and redneck trailer trash, not what is the proper (or even just plain decent) behavior of those who claim to be “freedom fighters.”

Most recently, there has been the conclusion of [Baez v. Rudkowski](#), Unanswered Indictment #120301, where the alleged founder of the political activist organization [We Are Change](#), **Luke Rudkowski**, was found, **under probable cause**, to have committed 2 counts of libel, 1 count of embezzlement, 1 count of extortion, and 2 counts of fraud. Apparently, this “leader” of the “leaderless” WAC was more than happy to lie with a straight face about how any and all donations were to go to one of two sources, neither of which was his own personal bank account, which ironically is where the all the monies ended up anyway. Whatever he may or may not have done after 2009 is unknown at this time, but it is certain though that he cleared a cool \$60,000 plus, starting in 2007. Everyone and anyone who crossed him, by simply asking for the financial records, was immediately demonized as a nutcase, and if they persisted, were blatantly accused of being not-so-undercover government agents. No trial, no jury, not even the faint equivalent of *habeas corpus*; just BANG!....discredited only by virtue of a baseless accusation without any proof. Sounds just like the same secret police game the Soviets played with their own citizens, doesn’t it?

As if that wasn’t bad enough, consider also the jurors who were negligent and/or uncommitted in their duties that *they voluntarily signed up for*. **Robert Handel** (alias Green Mountain Patriot) and **James Sims** (alias J Sims) both had to be placed on the CLC’s Wall of Shame for willfully failing to keep their commitments. Sims seems to be the worst of the two because he deliberately antagonized the Grand Jury Foreman, so at least Handel to his credit was considerate enough to at least be silently dishonorable. In one way, Handel reminds me of that juror from [The Moon is a Harsh Mistress](#) who negligently slept through a case he was supposed to be hearing (that juror was literally thrown out by the protagonist, Manuel O’Kelly, who was acting in the capacity of a judge).

And then there was **Mark Koenig** (alias Smiter13), who violated his Secrecy Oath that he willingly took when he volunteered to become a grand juror. Adding insult to injury, he completely lied about being strong-armed by government agents into sabotaging the *Baez v. Rudkowski* case by calling into [The Crotch Shot Radio Show](#) and baiting the host, **Louie Bee**. To top it all off, even [the Washington State Militia ended up relieving him of his command](#); in other words, they kicked him out on his ass.

Now, a common point of confusion [that comes up every time I'm interviewed about the CLC](#) are misunderstandings concerning its enforcement mechanism. Even thinking back on it, I am pretty appalled about how clearly different types of political dissidents are *still* absurdly ignorant regarding [the power of ostracism](#). Based on the liberty of association, ostracism is admitted by both libertarians and constitutionalists alike to be a peaceful way to deal with undesirables who seek to dominate and control others. Stefan Molyneux has said, "All we need to do is publish their crimes for all to see, and let the natural justice of society take care of the rest;" Gary Hunt takes in one step further by stating that, "It is time for us to be as serious about ridding ourselves of these subversive elements as we are about our individual causes, for all are doomed to failure unless we regain control of our own activities." Both men are absolutely correct about the need for dissidents of all kinds to choose their compatriots carefully, for as [the old adage goes](#), "You are judged by the company you keep."

If there ever was a truly serious effort at taking the genuine [alternative media](#) back from the [Carnival of Distractions](#), the CoS-CLC is *it*. By at least trying to act as a referee of sorts, the CLC is able to provide a neutral setting where each side can get a fair hearing. Upon completion of a case, the value of the CLC's findings carry weight within the Patriot Community because of its credibility. If somebody tries to spew sensationalistic bullshit that ends up harming someone else, then as long as a complaint is filed with the CLC, then there is a realistic chance the *real* truth will eventually come out.

According to [the old Chinese curse](#), "May you live in interesting times." Yeah, no kidding...with all these dopes, windbags, and shills (wittingly or unwittingly) trying to discredit, demoralize, and discourage political dissidents from attempting to secure the Liberty that is rightfully theirs, "interesting times" is the understatement of the decade. I can only hope more good people start taking whom they choose to associate with much more seriously. And who knows? Maybe a brick-and-mortar version of the CoS-CLC will spring out of its strictly digital incarnation and greatly improve from there. Only time will tell.

Afterword

I remember when Ed Snowden became a whistleblower three years ago. His entire goal was to tell the truth to the American people, hoping that by doing so they would dismantle the surveillance police state apparatus to the point where the limitations imposed by the Fourth Amendment to the United States Constitution were obeyed by the federal government. Snowden's greatest fear was that despite his noble sacrifice, Americans would apathetically disregard his warnings and continue to live out their lives, business as usual.

Although reform of the so-called "intelligence community" was all that Snowden was aiming for, even his task of spreading awareness fell embarrassingly flat. He took quite a daunting risk, and the payoff was less than stellar; for example, Christopher Greene, the American proprietor of AMTV (Alternative Media Television), has subsequently accused Snowden of being a "limited hangout," whereas John Oliver, a British progressive, was much kinder and quite sympathetic to Snowden's plight. I knew Snowden's revelations had been badly handicapped once I realized that I was siding with a welfare statist against a constitutionalist on this matter (interestingly enough, Greene has since endorsed Donald Trump's presidential campaign).

Thankfully, the crypto-anarchist resurgence in the wake of Snowden's disclosures has been maintained fairly well, for the most part. Despite my criticism regarding the lack of security audits for free and open-source cryptographic software, I still think that digital technology is still the best route in defeating indiscriminate surveillance. Applications that can be used to encrypt computer files and store them in a "cloud" are a likely powerful tool for libertarians, provided that strong cryptography and zero knowledge are used together for off-site data storage.

The era of disingenuous "activism" must end if human liberty is to be secured. As far as I am concerned, the Free State Project, the Second Amendment Foundation, the National Liberty Alliance, the Constitutional Sheriffs and Peace Officers Association, the Tenth Amendment Center, the Idaho Three Percenters, and the anti-libertarian "Libertarian" Party are not dissimilar from the *volksdeutchers* in Nazi-occupied Poland. Anti-activist "activist" organizations like those are filled with sell-outs of the worst kind, and it is because of their documented betrayals against their respective memberships that I recommend leaderless resistance and freedom cells as privacy-friendly alternatives, especially for those who genuinely consider themselves to be freedom activists.

Kyle Rearden
Austin, Texas
July 2016

Bibliography

A Primer on Security Culture

- <https://youtu.be/luvthTjC0OI>
- https://en.wikipedia.org/wiki/Security_culture
- https://en.wikipedia.org/wiki/Right_to_privacy
- https://en.wikipedia.org/wiki/Expectation_of_privacy
- https://en.wikipedia.org/wiki/Security_theater
- https://en.wikipedia.org/wiki/Civil_libertarianism
- <http://www.thelastbastille.com/2016/06/14/vonu-search-personal-freedom/>
- <http://www.thelastbastille.com/2015/07/16/reformism-does-not-work-a-critique-of-political-activism/>
- <http://www.libertyunderattack.com/luca-radio-6-5-16-das-17-survivalism/>
- <https://tinyurl.com/vonurayo>
- <https://youtu.be/UI7K2yXMucE>
- <https://en.wikipedia.org/wiki/Satyagraha>
- <http://www.thelastbastille.com/2014/07/19/ecodefense/>
- <http://www.libertyunderattack.com/assassination-politics-jim-bell/>
- <http://www.thelastbastille.com/2012/11/24/our-vanishing-privacy/>
- <http://www.privacyjournal.net/index.htm>
- <http://www.thelastbastille.com/2015/02/21/whos-watching-you/>
- <http://www.thelastbastille.com/2012/07/08/stealing-your-life/>
- <http://www.thelastbastille.com/2016/03/06/privacy-how-to-get-it-how-to-enjoy-it/>
- <http://www.thelastbastille.com/2013/09/06/rats/>
- <http://www.thelastbastille.com/2013/03/06/mind-your-own-business/>
- <http://www.thelastbastille.com/2015/07/03/the-end-of-america/>
- <http://tiny.cc/dragnetwiretapping>
- <https://tinyurl.com/emailkeywords>
- <http://tinyurl.com/cellphoneliberty>
- <http://www.thelastbastille.com/2016/05/22/dual-layer-encryption-proposal-sidestepping-potential-backdoors/>
- <http://tiny.cc/configurepgp4mac>
- <https://tiny.cc/socialistinsecurity>
- <http://tinyurl.com/never4getu>
- <http://tiny.cc/skepticism>

- <http://tiny.cc/doomporn>
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- <http://tinyurl.com/securedrecordarchival>
- <https://tinyurl.com/keepyourcounsel>
- <http://tiny.cc/chillingdissent>
- <http://tiny.cc/warningsign>
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <https://tinyurl.com/artofthegreyman>
- <https://tinyurl.com/inconspicuouscar>
- <http://www.thelastbastille.com/2016/06/22/home-hardening-fortify-domicile-intruders/>
- <http://tiny.cc/keepthepeace>
- <http://tiny.cc/leaderlessresistance>
- <http://tiny.cc/vetting>
- <https://tinyurl.com/mayulive>
- https://en.wikipedia.org/wiki/Free_and_open-source_software
- <http://www.thelastbastille.com/2012/07/27/pgp-pretty-good-privacy/>
- https://en.wikipedia.org/wiki/New_Deal
- <http://tiny.cc/grievances>
- <http://tiny.cc/newscycle>
- <http://www.nocards.org/press/overview.shtml>
- <https://epic.org/epic/about.html>
- <https://www.eff.org/about>
- <https://www.privacyrights.org/contact-us>
- <https://www.aclu.org/>
- <http://www.thelastbastille.com/2015/07/14/suing-the-government-does-not-work-lawsuits-are-not-useful-for-securing-your-liberty/>
- <https://www.aclu.org/issues/lgbt-rights/lgbt-nondiscrimination-protections>
- <https://www.aclu.org/issues/hiv/hivaids-and-discrimination>
- <https://www.aclu.org/issues/national-security/privacy-and-surveillance>
- <https://www.aclu.org/issues/free-speech/freedom-press>
- <https://www.aclu.org/issues/national-security/secrecy>
- <https://www.aclu.org/issues/privacy-technology/internet-privacy>
- <https://www.aclu.org/issues/privacy-technology/medical-and-genetic-privacy>
- <https://www.aclu.org/issues/privacy-technology/workplace-privacy>

- <https://www.privacyrights.org/Privacy-Rights-Fact-Sheets>
- <https://www.privacyrights.org/privacy-survival-take-control-your-personal-information>
- <https://www.privacyrights.org/wireless-communications-voice-and-data-privacy>
- <https://www.privacyrights.org/content/how-put-end-unwanted-or-harassing-phone-calls>
- <https://www.privacyrights.org/junk-mail-how-did-they-all-get-my-address>
- <https://www.privacyrights.org/telemarketing-how-have-quiet-evening-home>
- <https://www.privacyrights.org/how-private-my-credit-report>
- <https://www.privacyrights.org/workplace-privacy-and-employee-monitoring>
- <https://www.privacyrights.org/content/introduction-health-and-medical-information-privacy>
- <https://www.privacyrights.org/content/wiretapping-and-eavesdropping-telephone-calls>
- <https://www.privacyrights.org/my-social-security-number-how-secure-it>
- <https://www.privacyrights.org/cradle-grave-government-records-and-your-privacy>
- <https://www.privacyrights.org/checklist-responsible-information-handling-practices>
- <https://www.privacyrights.org/are-you-being-stalked>
- <https://www.privacyrights.org/what-personal-information-should-you-give-merchants>
- <https://www.privacyrights.org/employment-background-checks-jobseekers-guide>
- <https://tinyurl.com/freeganismprimer>
- <http://tinyurl.com/lualrm2>
- <http://www.libertyunderattack.com/recommended-articles/>
- <http://www.libertyunderattack.com/security-culture/>
- <http://www.libertyunderattack.com/kyle-reardens-book-reports/>
- <http://www.libertyunderattack.com/solutions/>

A History of Dragnet Wiretapping

- https://en.wikipedia.org/wiki/State_secrets_privilege
- <https://en.wikipedia.org/wiki/Omniscience>
- [https://en.wikipedia.org/wiki/Panopticon#Criticism_and_the_Panoptic on as metaphor](https://en.wikipedia.org/wiki/Panopticon#Criticism_and_the_Panoptic_on_as_metaphor)
- <http://youtu.be/C8EcrnEmNcc?t=5m55s>
- https://en.wikipedia.org/wiki/Joseph_Fouch%C3%A9
- [https://en.wikipedia.org/wiki/Jos%C3%A9_Gaspar_Rodr%C3%ADguez de Francia](https://en.wikipedia.org/wiki/Jos%C3%A9_Gaspar_Rodr%C3%ADguez_de_Francia)
- <https://en.wikipedia.org/wiki/Securitate>
- <https://en.wikipedia.org/wiki/Eavesdropping>
- <http://people.howstuffworks.com/wiretapping1.htm/printable>
- <http://electronics.howstuffworks.com/telephone.htm/printable>
- <http://electronics.howstuffworks.com/cordless-telephone.htm/printable>
- <http://electronics.howstuffworks.com/cell-phone.htm/printable>
- <http://electronics.howstuffworks.com/gadgets/travel/satellite-phone.htm/printable>
- <http://electronics.howstuffworks.com/ham-radio.htm/printable>
- <http://computer.howstuffworks.com/ip-telephony.htm/printable>
- <http://www.mesinnovations.com/devices/telegwiretaps.html>
- https://www.nsa.gov/public_info/_files/truman/truman_memo.pdf
- https://en.wikipedia.org/wiki/Signals_intelligence
- https://en.wikipedia.org/wiki/Church_Committee
- [http://www.aarclibrary.org/publib/church/reports/book2/pages/Church B2_0062b.gif](http://www.aarclibrary.org/publib/church/reports/book2/pages/Church_B2_0062b.gif)
- [http://www.aarclibrary.org/publib/church/reports/book2/pages/Church B2_0011a.gif](http://www.aarclibrary.org/publib/church/reports/book2/pages/Church_B2_0011a.gif)
- <http://www.thelastbastille.com/2012/01/17/911-synthetic-terror/>
- https://en.wikipedia.org/wiki/United_States_Intelligence_Community
- https://en.wikipedia.org/wiki/War_on_Terror
- <http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/107994/major-general-mark-o-schissler.aspx>
- <https://www.wsws.org/en/articles/2006/12/gene-d19.html>
- <http://www.thelastbastille.com/2012/05/14/who-are-the-terrorists/>
- https://en.wikipedia.org/wiki/Unreasonable_search_and_seizure
- https://en.wikipedia.org/wiki/Article_Two_of_the_United_States_Constitution#Clause_1:_Command_of_military.3B_Opinions_of_cabinet_secretaries.3B_Pardons

- [https://en.wikipedia.org/wiki/Executive_Office_of_the_President_of the United States](https://en.wikipedia.org/wiki/Executive_Office_of_the_President_of_the_United_States)
- [https://en.wikipedia.org/wiki/Article_One_of_the_United_States_Constitution#Section 8: Powers of Congress](https://en.wikipedia.org/wiki/Article_One_of_the_United_States_Constitution#Section_8:_Powers_of_Congress)
- <http://youtu.be/cGhcECnWRGM>
- https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act
- https://en.wikipedia.org/wiki/Project_MINARET
- <http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court>
- [https://en.wikipedia.org/wiki/Communications_Assistance_for_Law Enforcement Act](https://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act)
- https://en.wikipedia.org/wiki/Backdoor_%28computing%29
- <https://www.eff.org/issues/calea>
- https://en.wikipedia.org/wiki/Patriot_Act
- https://en.wikipedia.org/wiki/Roving_wiretap
- <https://epic.org/privacy/terrorism/usapatriot/#analysis>
- [https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act of 1978 Amendments Act of 2008](https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008)
- https://en.wikipedia.org/wiki/Stellar_Wind
- <http://openjurist.org/277/us/438>
- <http://openjurist.org/389/us/347>
- <http://www.thelastbastille.com/2014/02/17/the-etymology-of-the-word-anarchy/>
- <http://openjurist.org/407/us/297>
- [https://en.wikipedia.org/wiki/United_States_v._United_States_District Court](https://en.wikipedia.org/wiki/United_States_v._United_States_District_Court)
- [https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States Constitution#Warrant](https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution#Warrant)
- [https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States Constitution#Exceptions_to_the_warrant_requirement](https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution#Exceptions_to_the_warrant_requirement)
- <http://www.katzjustice.com/tomero.pdf>
- https://en.wikipedia.org/wiki/Roving_wiretap
- <http://www.ca6.uscourts.gov/opinions.pdf/07a0253p-06.pdf>
- https://www.eff.org/files/filenode/20111229_9c_hepting_opinion.pdf
- <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title50/html/USCODE-2012-title50-chap36-subchapVII-sec1885a.htm>
- <http://www.gpo.gov/fdsys/pkg/USCOURTS-ca9-10-30126/pdf/USCOURTS-ca9-10-30126-0.pdf>
- <https://ia601403.us.archive.org/22/items/gov.uscourts.cand.207206/gov.uscourts.cand.207206.321.0.pdf>

- https://en.wikipedia.org/wiki/Room_641A
- https://en.wikipedia.org/wiki/Mark_Klein
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- <http://www.thelastbastille.com/2015/02/21/whos-watching-you/>
- https://en.wikipedia.org/wiki/Five_Eyes
- https://en.wikipedia.org/wiki/Secret_treaty
- https://en.wikipedia.org/wiki/UKUSA_Agreement
- https://en.wikipedia.org/wiki/Article_Two_of_the_United_States_Constitution#Clause_2:_Advice_and_Consent_Clause
- https://en.wikipedia.org/wiki/Temporary_Committee_on_the_ECHEL_ON_Interception_System
- https://en.wikipedia.org/wiki/Communications_Security_Establishment
- https://en.wikipedia.org/wiki/Government_Communications_Headquarters
- https://en.wikipedia.org/wiki/Australian_Signals_Directorate
- https://en.wikipedia.org/wiki/Government_Communications_Security_Bureau
- http://www.wired.com/2012/03/ff_nsadatacenter/all/
- http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm
- https://upload.wikimedia.org/wikipedia/commons/f/f3/PRISM_Collection_Details.jpg
- <https://upload.wikimedia.org/wikipedia/commons/thumb/0/00/NSA-MUSCULAR-p22.png/640px-NSA-MUSCULAR-p22.png>
- https://en.wikipedia.org/wiki/Black_room
- https://en.wikipedia.org/wiki/Perry_Fellwock
- https://en.wikipedia.org/wiki/Russ_Tice
- https://en.wikipedia.org/wiki/Thomas_Tamm
- https://en.wikipedia.org/wiki/William_Binney_%28U.S._intelligence_official%29
- https://en.wikipedia.org/wiki/Thomas_Andrews_Drake
- https://en.wikipedia.org/wiki/Edward_Snowden
- https://en.wikipedia.org/wiki/Limited_hangout
- https://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf
- https://en.wikipedia.org/wiki/Omnibus_Crime_Control_and_Safe_Streets_Act_of_1968

- https://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act
- https://en.wikipedia.org/wiki/Enemy_of_the_State_%28film%29
- <http://object.cato.org/sites/cato.org/files/serials/files/regulation/2004/10/v27n3-5.pdf>
- <http://www.nytimes.com/2005/12/16/politics/16program.html>
- http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
- <https://en.wikipedia.org/wiki/Reformism>
- <http://www.thelastbastille.com/2014/04/26/administrative-agencies-the-fourth-branch-of-government/>
- <https://en.wikipedia.org/wiki/Cypherpunk>
- <https://en.wikipedia.org/wiki/Crypto-anarchism>
- https://en.wikipedia.org/wiki/Crypto_wars
- https://en.wikipedia.org/wiki/Free_and_open-source_software
- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://en.wikipedia.org/wiki/End-to-end_encryption
- https://en.wikipedia.org/wiki/Secure_telephone
- <http://www.thelastbastille.com/2013/01/18/how-to-configure-use-gpg-encryption-for-email-mac-osx-instructions/>
- <http://www.thelastbastille.com/2015/02/06/how-to-configure-use-otr-encryption-for-instant-messaging-on-skype-mac-osx-tutorial/>
- <https://en.wikipedia.org/wiki/ZRTP>
- <http://www.thelastbastille.com/2014/03/19/they-dont-make-em-like-they-used-to/>
- <http://www.committee.org/faq.htm>
- <http://youtu.be/KQLy012pNDs?t=2m34s>
- <http://www.thefreedictionary.com/lead+balloon>
- <http://www.thelastbastille.com/2012/10/15/the-new-world-order/>
- <http://outpost-of-freedom.com/blog/?p=540>
- <http://www.activism.net/cypherpunk/manifesto.html>
- http://youtu.be/Wj7IksIf_JI

Data-mining the Haystack: Should You Attempt to Overload the NSA's Servers with "Suspicious" Email Keywords?

- <http://youtu.be/KQLy012pNDs?t=2m4s>
- https://en.wikipedia.org/wiki/Data_mining

- <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title50/html/USCODE-2013-title50-chap36-subchapIV-sec1861.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm>
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>
- <http://www.thelastbastille.com/2015/03/02/a-history-of-dragnet-wiretapping/>
- <http://info.publicintelligence.net/UtahDataCenter.pdf>
- https://en.wikipedia.org/wiki/Temporary_Committee_on_the_ECHEL_ON_Interception_System
- https://en.wikipedia.org/wiki/Five_Eyes
- https://en.wikipedia.org/wiki/UKUSA_Agreement
- http://www.wired.com/2012/03/ff_nsadatacenter/all/1
- http://www.msco.mil/documents/_7_GIG%20Architectural%20Vision%20-%20200706%20v1.0.pdf
- <https://en.wikipedia.org/wiki/Yottabyte>
- <https://en.wikipedia.org/wiki/Terabytes>
- <http://www.thelastbastille.com/2015/07/16/reformism-does-not-work-a-critique-of-political-activism/>
- https://en.wikipedia.org/wiki/FISA_Amendments_Act
- [https://en.wikipedia.org/wiki/PRISM_\(surveillance_program\)](https://en.wikipedia.org/wiki/PRISM_(surveillance_program))
- [https://en.wikipedia.org/wiki/MUSCULAR_\(surveillance_program\)](https://en.wikipedia.org/wiki/MUSCULAR_(surveillance_program))
- <https://en.wikipedia.org/wiki/XKeyscore>
- https://en.wikipedia.org/wiki/Internet_backbone
- <http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents>
- https://en.wikipedia.org/wiki/Government_Communications_Headquarters
- https://en.wikipedia.org/wiki/Communications_Security_Establishment
- https://en.wikipedia.org/wiki/Australian_Signals_Directorate
- https://en.wikipedia.org/wiki/Government_Communications_Security_Bureau
- http://www.pcworld.com/article/249137/what_is_deep_packet_inspection.html
- https://en.wikipedia.org/wiki/State_secrets_privilege
- <https://youtu.be/oYNXVgYhPOc>
- https://en.wikipedia.org/wiki/Edward_Snowden

- <http://www.wired.com/2012/03/nsa-denies-wired/>
- <https://youtu.be/rENTl5JKzIQ?t=1m44s>
- <https://youtu.be/rENTl5JKzIQ?t=3m56s>
- <https://youtu.be/rENTl5JKzIQ?t=8m7s>
- <http://attrition.org/misc/keywords.html>
- <http://nsa.motherboard.tv/>
- <http://www.popsci.com/technology/article/2013-06/vice-creates-spam-generator-befuddle-nsa>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/analysts_desktop_binder_redacted_dhs.pdf
- <http://trollthensa.com/>
- https://en.wikipedia.org/wiki/Critical_mass_%28sociodynamics%29
- http://email.about.com/od/emailstatistics/f/What_is_the_Average_Size_of_an_Email_Message.htm
- <https://youtu.be/S5PvBzDlZGs>
- https://en.wikipedia.org/wiki/Black_fax
- <http://www.thelastbastille.com/2012/07/27/pgp-pretty-good-privacy/>
- <http://www.thelastbastille.com/2013/03/25/how-to-configure-use-pgp-encryption-for-email-windows-os-instructions/>
- <http://www.thelastbastille.com/2013/01/18/how-to-configure-use-pgp-encryption-for-email-mac-osx-instructions/>
- <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN>
- <http://www.gnupg.org/>
- <http://www.thelastbastille.com/2015/11/28/bitcoiners-betrayed-lobbyists-sell-out-to-the-government/>
- https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy
- <http://www.libertyunderattack.com/solutions/>

Are Cellular Telephones Furthering Human Liberty?

- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>
- <http://www.libertyunderattack.com/anonymous-encrypted-phones/>
- https://en.wikipedia.org/wiki/Off-the-Record_Messaging
- <https://en.wikipedia.org/wiki/ZRTP>
- <http://www.libertyunderattack.com/security-culture/>
- https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution
- <http://tiny.cc/dragnetwiretapping>

- https://en.wikipedia.org/wiki/Right_to_keep_and_bear_arms
- https://en.wikipedia.org/wiki/Freedom_of_assembly
- <http://www.katzjustice.com/tomero.pdf>
- <https://www.gpo.gov/fdsys/pkg/USCOURTS-ca7-10-03803/pdf/USCOURTS-ca7-10-03803-1.pdf>
- <http://www.gpo.gov/fdsys/pkg/USCOURTS-ca9-10-30126/pdf/USCOURTS-ca9-10-30126-0.pdf>
- <http://www.ca6.uscourts.gov/opinions.pdf/12a0262p-06.pdf>
- <https://en.wikipedia.org/wiki/Geolocation>
- <http://www.leagle.com/decision/In%20FDCO%2020130508G77/U.S.%20v.%20RIGMAIDEN>
- <http://www.leagle.com/decision/In%20FDCO%2020130828799/U.S.%20v.%20RIGMAIDEN>
- <https://www.eff.org/files/filenode/08-90330.pdf>
- http://www.supremecourt.gov/orders/courtorders/011116zor_n7io.pdf
- <http://www2.epic.org/foia/dhs/internet-kill-switch/Cert-Petition.pdf>
- <http://www2.epic.org/foia/dhs/internet-kill-switch/default.html>
- https://en.wikipedia.org/wiki/Attorney%E2%80%93client_privilege
- https://en.wikipedia.org/wiki/Fifth_Amendment_to_the_United_States_Constitution#Self-incrimination
- https://en.wikipedia.org/wiki/Omnibus_Crime_Control_and_Safe_Streets_Act_of_1968
- <http://www.leagle.com/decision/In%20FDCO%2020130508G77/U.S.%20v.%20RIGMAIDEN>
- https://en.wikipedia.org/wiki/Color_law
- https://en.wikipedia.org/wiki/Fruit_of_the_poisonous_tree
- <http://openjurist.org/998/f2d/1112>
- <http://www.thelastbastille.com/2013/11/08/common-law-legally-defined/>
- <http://www.heritage.org/constitution/amendments/4/essays/145/warrant-clause>
- <http://openjurist.org/277/us/438>
- <http://www.uscourts.gov/statistics-reports/wiretap-report-2012>
- <http://www.uscourts.gov/statistics-reports/wiretap-report-2013>
- <http://www.uscourts.gov/statistics-reports/wiretap-report-2014>
- <http://www.libertyunderattack.com/anonymous-encrypted-phones/>
- <http://ia601409.us.archive.org/28/items/gov.uscourts.vaed.321610/gov.uscourts.vaed.321610.7.0.pdf>
- <https://tinyurl.com/keepyourcounsel>

- https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute
- http://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html?_r=0
- https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html
- <https://www.washingtonpost.com/news/post-nation/wp/2016/04/07/fbi-director-says-method-for-unlocking-san-bernardino-iphone-only-works-on-narrow-slice-of-devices/>
- <https://www.eff.org/deeplinks/2014/11/jailbreaking-not-crime-and-eff-fighting-keep-it-way>
- https://www.eff.org/files/filenode/dmca_2009/rm-2008-8.pdf
- https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29#/media/File:Prism_slide_5.jpg
- https://en.wikipedia.org/wiki/Free_and_open-source_software
- <http://www.wthr.com/Global/story.asp?S=9346833>
- <https://en.wikipedia.org/wiki/Cellebrite>
- <http://www.cellebrite.com/Media/Default/Files/Forensics/Solution-Briefs/Mobile-Forensics-Solution-Brief.pdf>
- https://en.wikipedia.org/wiki/Data_extraction
- https://en.wikipedia.org/wiki/Carl_Cameron
- <https://youtu.be/H20Naj176M0>
- https://en.wikipedia.org/wiki/Free_software
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- https://en.wikipedia.org/wiki/Spontaneous_order
- https://en.wikipedia.org/wiki/Market_discipline
- <https://youtu.be/1RVqnIuH6hI>
- <http://www.thelastbastille.com/2014/07/09/i-pencil/>
- https://en.wikipedia.org/wiki/Price_system
- https://en.wikipedia.org/wiki/Use_value
- https://en.wikipedia.org/wiki/Cordless_telephone
- https://en.wikipedia.org/wiki/Car_phone
- <https://en.wikipedia.org/wiki/Demand>
- <https://en.wikipedia.org/wiki/Neo-Luddism>
- https://en.wikipedia.org/wiki/Latchkey_kid
- [https://en.wikipedia.org/wiki/Uber_\(company\)](https://en.wikipedia.org/wiki/Uber_(company))
- https://en.wikipedia.org/wiki/End-to-end_encryption

- https://en.wikipedia.org/wiki/Legal_status_of_Uber's_service
- https://en.wikipedia.org/wiki/Information_technology_security_audit
- <https://en.wikipedia.org/wiki/Moneybomb>
- <http://anagram.com/berson/abskyeval.html>
- https://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29#/media/File:Prism_slide_5.jpg
- <https://en.wikipedia.org/wiki/Crowdfunding>
- <http://tiny.cc/legaldefensefundscam>
- <https://en.wikipedia.org/wiki/Meta-analysis>
- <http://www.sciencedirect.com/science/article/pii/S2213879X14000583>
- https://en.wikipedia.org/wiki/Confirmation_bias
- https://en.wikipedia.org/wiki/Electromagnetic_radiation_and_health
- <http://www.pewinternet.org/2011/02/03/generations-and-their-gadgets/>
- <http://www.pewinternet.org/2011/08/15/americans-and-their-cell-phones/>
- <http://www.alternet.org/culture/why-rude-cell-phone-users-have-won>
- <http://tiny.cc/grievances>
- <http://researchnews.osu.edu/archive/distractwalk.htm>
- <https://en.wikipedia.org/wiki/Luddite>
- <https://prism-break.org/en/protocols/otr>
- <https://prism-break.org/en/protocols/zrtp>
- <https://prism-break.org/en/>
- <https://ssd.eff.org/>
- <https://securityinabox.org/>
- <https://www.privacyrights.org/privacy-rights-fact-sheets>
- <https://blackphone.ch/>
- <https://zomiaofflinegames.com/darkandroid/>
- <http://www.cryptophone.de/en/>
- <https://www.fsf.org/>
- <https://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf>
- <http://www.thelastbastille.com/2016/06/05/montographs-cellular-telephone-demonstrations/>
- http://www.wrc.noaa.gov/wrso/security_guide/cellular.htm
- https://youtu.be/Ouo7Q6Cf_yc

Dual Layer Encryption: A Proposal for Sidestepping Potential Backdoors

- http://www.rossde.com/PGP/pgp_backdoor.html
- https://en.wikipedia.org/wiki/Phil_Zimmermann
- <https://www.philzimmermann.com/EN/faq/index.html>
- <https://tinyurl.com/emailkeywords>
- <http://www.thelastbastille.com/2012/07/27/pgp-pretty-good-privacy/>
- <http://tiny.cc/configurepgp4mac>
- https://en.wikipedia.org/wiki/Free_and_open-source_software
- http://outpost-of-freedom.com/blog/?page_id=6
- <http://outpost-of-freedom.com/blog/?p=540>
- https://en.wikipedia.org/wiki/Multiple_encryption
- https://en.wikipedia.org/wiki/Classical_cipher
- <https://prism-break.org/en/protocols/gpg/>
- <https://prism-break.org/en/protocols/otr/>
- <https://prism-break.org/en/protocols/zrtp/>
- https://en.wikipedia.org/wiki/Transposition_cipher
- https://en.wikipedia.org/wiki/Substitution_cipher
- https://en.wikipedia.org/wiki/One-time_pad
- <https://en.wikipedia.org/wiki/Plaintext>
- <https://en.wikipedia.org/wiki/Ciphertext>
- https://en.wikipedia.org/wiki/Caesar_cipher
- https://en.wikipedia.org/wiki/Proof_of_concept
- <https://tinyurl.com/keepyourcounsel>
- https://en.wikipedia.org/wiki/Public-key_cryptography
- <http://tiny.cc/dragnetwiretapping>
- <http://www.thelastbastille.com/2012/12/03/how-to-hide-things-in-public-places/>
- https://en.wikipedia.org/wiki/White_hat_%28computer_security%29
- <http://www.cryptogram.org/about.html>
- https://en.wikipedia.org/wiki/Single_point_of_failure
- kyle@thelastbastille.com

How to Configure & Use PGP Encryption for Email

- <http://www.thelastbastille.com/2012/07/27/pgp-pretty-good-privacy/>
- <http://www.thelastbastille.com/2012/08/11/the-internet/>
- https://en.wikipedia.org/wiki/Public-key_cryptography

- https://en.wikipedia.org/wiki/Pretty_Good_Privacy#Criminal_investigation
- https://en.wikipedia.org/wiki/Export_of_cryptography_in_the_United_States#PC_era
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- https://en.wikipedia.org/wiki/Apple_Inc.
- <http://www.gnupg.org/>
- https://en.wikipedia.org/wiki/Free_and_open_source_software
- https://en.wikipedia.org/wiki/Pretty_Good_Privacy#OpenPGP
- <https://www.fsf.org/about/>
- https://en.wikipedia.org/wiki/Mozilla_Thunderbird
- <https://en.wikipedia.org/wiki/Enigmail>
- <http://www.thelastbastille.com/2013/03/25/how-to-configure-use-gpg-encryption-for-email-windows-os-instructions/>
- https://en.wikipedia.org/wiki/Comparison_of_webmail_providers
- <https://www.mozilla.org/en-US/thunderbird>
- https://en.wikipedia.org/wiki/Menu_bar
- <https://www.gpgtools.org/>
- <https://en.wikipedia.org/wiki/Passphrase>
- <http://support.gpgtools.org/kb/how-to/first-steps-where-do-i-start-where-do-i-begin>
- https://en.wikipedia.org/wiki/USB_flash_drive
- kyle@thelastbastille.com
- <https://youtu.be/yXm0dtYFxZk>
- <https://youtu.be/Rt4MFkbr6co>
- <https://youtu.be/oHEWVIynQ8Q>

How to Configure & Use Jitsi (Windows OS)

- <https://jitsi.org/>
- <https://duck.co/blog/xmpp-services-at-duckduckgo>
- <https://youtu.be/udBBDHT-UA>
- <https://youtu.be/vgx7VSrDGjk>
- <http://www.libertyunderattack.com/wp-content/uploads/Documents/How%20To%20Encrypt%20Chat%20And%20VoIP%20With%20Jitsi%20&%20XMPP%20-%20Pillow%20Fortress%20blog.pdf>
- shane@libertyunderattack.com

- <http://www.thelastbastille.com/2013/03/25/how-to-configure-use-pgp-encryption-for-email-windows-os-instructions/>

Socialist Insecurity: How the Raw Deal Enslaved Americans

- <http://www.thelastbastille.com/2013/02/06/a-law-unto-itself/>
- <http://www.thelastbastille.com/2013/02/27/a-primer-on-welfare-statism-why-you-should-never-accept-a-government-handout/>
- <http://www.thelastbastille.com/2012/07/09/balkanization/>
- https://en.wikipedia.org/wiki/Social_Security_%28United_States%29
- <http://www.thelastbastille.com/2011/12/31/problem-reaction-solution-hegelian-dialectic/>
- https://en.wikipedia.org/wiki/Hanlon's_razor
- https://en.wikipedia.org/wiki/Social_insurance
- <http://www.thelastbastille.com/2012/10/04/fractional-reserve-lending/>
- https://en.wikipedia.org/wiki/Financial_crisis
- https://en.wikipedia.org/wiki/Second_Bank_of_the_United_States
- https://en.wikipedia.org/wiki/Panic_of_1819
- https://en.wikipedia.org/wiki/Panic_of_1907
- http://wiki.mises.org/wiki/Panic_of_1907
- <https://tinyurl.com/endingwar>
- <http://www.thelastbastille.com/2012/09/24/the-creature-from-jekyll-island/>
- <https://en.wikipedia.org/wiki/Malinvestment>
- https://en.wikipedia.org/wiki/Wall_Street_Crash_of_1929
- https://en.wikipedia.org/wiki/Austrian_business_cycle_theory
- https://en.wikipedia.org/wiki/Credit_creation
- https://en.wikipedia.org/wiki/Credit_crunch
- <http://www.thelastbastille.com/2015/12/21/quote-of-the-week-regarding-the-great-depression/>
- <https://www.mises.ca/stalins-apologists>
- https://en.wikipedia.org/wiki/Social_Security_Act
- https://en.wikipedia.org/wiki/Franklin_D._Roosevelt
- https://en.wikipedia.org/wiki/Social_Security_number
- https://en.wikipedia.org/wiki/Social_Security_Trust_Fund
- <http://www.thelastbastille.com/2014/04/26/administrative-agencies-the-fourth-branch-of-government/>
- https://en.wikipedia.org/wiki/Preamble_to_the_United_States_Constitution#Text

- https://en.wikipedia.org/wiki/Taxing_and_Spending_Clause#Constitutional_text
- <http://www.thelastbastille.com/2015/12/09/are-you-obligated-to-register-for-the-draft/>
- http://www.outpost-of-freedom.com/verbnd.htm#Charity,_Welfare,_General_Welfare
- https://en.wikipedia.org/wiki/James_Madison
- <http://www.thelastbastille.com/2013/06/23/the-federalist-papers/>
- <https://tinyurl.com/nullifythejury>
- <http://www.thelastbastille.com/2015/11/08/limited-carjacking-a-simile/>
- <http://1828.mshaffer.com/d/search/word,welfare>
- https://en.wikipedia.org/wiki/War_of_1812
- <http://www.thelastbastille.com/2013/07/12/the-anti-federalist-papers/>
- https://en.wikipedia.org/wiki/Plenary_power#United_States
- <https://fee.org/freeman/the-power-to-tax-is-the-power-to-destroy/>
- http://www.heritage.org/constitution/?_escaped_fragment_=/articles/1/essays/36/borrowing-clause#!/articles/1/essays/36/borrowing-clause
- https://en.wikipedia.org/wiki/United_States_debt_ceiling
- <http://www.ssa.gov/>
- <http://legislink.org/us/pl-74-271>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title26/html/USCODE-2013-title26-subtitleC-chap21.htm>
- <https://www.ssa.gov/history/briefhistory3.html>
- [https://en.wikipedia.org/wiki/Social_Security_\(United_States\)](https://en.wikipedia.org/wiki/Social_Security_(United_States))
- <http://openjurist.org/297/us/1>
- https://en.wikipedia.org/wiki/General_welfare_clause#Historical_Debate_and_Pre-1936_Rulings
- <http://openjurist.org/301/us/619>
- <https://en.wikipedia.org/wiki/Precedent#Principle>
- <http://openjurist.org/363/us/603>
- <http://www.socialsecurity.gov/policy/docs/ssb/v50n1/v50n1p5.pdf>
- https://en.wikipedia.org/wiki/Supremacy_Clause
- https://en.wikipedia.org/wiki/Tenth_Amendment_to_the_United_States_Constitution
- https://en.wikipedia.org/wiki/Judicial_Procedures_Reform_Bill_of_1937
- https://en.wikipedia.org/wiki/Ashwander_rules
- https://en.wikipedia.org/wiki/Judicial_review
- https://en.wikipedia.org/wiki/Constitutional_avoidance

- https://commons.wikimedia.org/wiki/File:Historical_Payroll_Tax_Rates.jpg
- https://en.wikipedia.org/wiki/Federal_Insurance_Contributions_Act_tax#/media/File:Share_of_Federal_Revenue_from_Different_Tax_Sources_%28Individual_Payroll_and_Corporate%29_1950_-_2010.gif
- https://en.wikipedia.org/wiki/Government_shutdown_in_the_United_States
- https://en.wikipedia.org/wiki/United_States_federal_government_credit-rating_downgrades
- <http://financial-dictionary.thefreedictionary.com/Unfunded+Liability>
- https://en.wikipedia.org/wiki/United_States_debt-ceiling_crisis_of_2011
- https://en.wikipedia.org/wiki/United_States_debt-ceiling_crisis_of_2013
- https://en.wikipedia.org/wiki/United_States_federal_government_shutdown_of_2013
- https://en.wikipedia.org/wiki/United_States_federal_government_shutdowns_of_1995%E2%80%931996
- https://en.wikipedia.org/wiki/National_debt_of_the_United_States#/media/File:USDebt.png
- <http://www.treasurydirect.gov/NP/debt/current>
- <http://www.ssa.gov/oact/tr/index.html>
- <http://www.backwoodshome.com/columns/duffy010223.html>
- <https://www.cbo.gov/publication/44972>
- <http://fas.org/sgp/crs/misc/RL33028.pdf>
- <https://youtu.be/5hkLaBiavqQ?t=2m2s>
- <https://youtu.be/rCdgv7n9xCY>
- https://en.wikipedia.org/wiki/Currency_war
- https://en.wikipedia.org/wiki/Sovereign_default
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- <https://www.ssa.gov/oact/tr/2015/index.html>
- https://en.wikipedia.org/wiki/Poverty_thresholds_%28United_States_Census_Bureau%29
- <http://apps.who.int/gho/data/node.main.688?lang=en>
- <https://youtu.be/F8rFjcsmo7s>
- <https://youtu.be/EwogDPh-Sow>
- <https://www.ssa.gov/news/press/factsheets/colafacts2016.html>
- <http://ericpetersautos.com/2015/12/09/drivers-license-and-social-security-number-please/>

- <http://www.bjs.gov/content/pub/press/vit08pr.cfm>
- <http://www.bjs.gov/content/pub/press/vit14pr.cfm>
- <http://www.bjs.gov/content/pub/press/vit12pr.cfm>
- <http://www.thelastbastille.com/2015/12/23/charles-mullens-1998-social-security-administration-letter/>
- <http://www.backwoodshome.com/columns/wolfe0310.html>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2014-title26/html/USCODE-2014-title26-subtitleF-chap61-subchapB-sec6109.htm>
- <https://www.gpo.gov/fdsys/pkg/CFR-2014-title26-vol18/pdf/CFR-2014-title26-vol18-part301.pdf>
- <https://www.ssa.gov/pubs/EN-05-10023.pdf>
- <http://www.backwoodshome.com/blogs/ClaireWolfe/2015/01/07/i-cant-help-you-with-that/>
- <http://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf>
- <http://www.thelastbastille.com/2015/12/28/dorcas-hardys-1986-social-security-letter/>
- http://www.lifescrypt.com/well-being/articles/t/the_right_to_refuse_service_or_discrimination.aspx
- https://en.wikipedia.org/wiki/Know_your_customer
- <http://www.gao.gov/products/GAO-04-11>
- https://en.wikipedia.org/wiki/Slippery_slope
- https://en.wikipedia.org/wiki/Captive_market
- https://en.wikipedia.org/wiki/Consumer_protection
- <http://www.thelastbastille.com/2015/07/16/reformism-does-not-work-a-critique-of-political-activism/>
- https://en.wikipedia.org/wiki/Soft_target
- <https://youtu.be/RjipR4qLups>
- <https://socialsecurity.gov/forms/ssa-521.pdf>
- <https://socialsecurity.gov/forms/ss-5.pdf>
- <http://www.thelastbastille.com/2014/02/03/only-on-paper-the-patetic-story-of-commerical-redemption-freemen-on-the-land-sovereign-citizens-lawful-rebellion-community-immunity/>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title5/html/USCODE-2013-title5-partI-chap5-subchapII-sec552a.htm>
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/html/USCODE-2013-title42-chap7-subchapII-sec405.htm>

- <http://www.thelastbastille.com/2015/07/14/suing-the-government-does-not-work-lawsuits-are-not-useful-for-securing-your-liberty/>
- <http://www.libertyunderattack.com/patriot-mythology-a-five-part-series/>
- <http://www.thelastbastille.com/2013/09/26/reborn-in-canada/>
- <http://www.thelastbastille.com/2012/10/03/on-the-duty-of-civil-disobedience/>
- <https://www.gpo.gov/fdsys/pkg/CFR-2014-title26-vol18/pdf/CFR-2014-title26-vol18-part301.pdf>
- https://youtu.be/TC_uHYbaADs
- <https://youtu.be/3Wt1ZjXv8Lg>
- <http://www.backwoodshome.com/blogs/ClaireWolfe/2015/01/07/i-cant-help-you-with-that/>
- <http://www.backwoodshome.com/columns/wolfe0310.html>
- <https://en.wikipedia.org/wiki/Subsidy#subsidies>
- <http://www.thelastbastille.com/2014/07/09/i-pencil/>
- https://en.wikipedia.org/wiki/Human_Action
- <https://youtu.be/F8rFjcsmo7s>
- <http://www.thelastbastille.com/2013/02/27/a-primer-on-welfare-statism-why-you-should-never-accept-a-government-handout/>
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- https://en.wikipedia.org/wiki/Nazi_Party
- <http://www.historyplace.com/worldwar2/riseofhitler/25points.htm>
- <http://www.thelastbastille.com/2013/02/27/a-primer-on-welfare-statism-why-you-should-never-accept-a-government-handout/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://www.thelastbastille.com/2012/11/24/our-vanishing-privacy/>
- <http://www.thelastbastille.com/2015/07/30/a-primer-on-homeschooling-how-to-resist-centrally-planned-indoctrination/>
- <https://www.privacyrights.org/my-social-security-number-how-secure-it>
- <http://www.thelastbastille.com/2013/02/06/a-law-unto-itself/>
- <http://www.thevoluntarylife.com/2013/09/124-four-ways-to-quit-rat-race.html>
- <http://www.thelastbastille.com/2015/12/22/thomas-jefferson-thought-every-generation-pay-debts/>
- <http://www.libertyunderattack.com/jumping-the-minarchist-ship-why-how-america-came-to-be/>

- <https://youtu.be/IFl9GsE5Mfg>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>

Do You Have the “Right” To be Forgotten?

- <http://www.thelastbastille.com/2012/12/19/1984/>
- <http://www.thelastbastille.com/2013/03/06/mind-your-own-business/>
- <https://tinyurl.com/keepyourcounsel>
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- https://en.wikipedia.org/wiki/Market_discipline
- https://en.wikipedia.org/wiki/Price_system
- https://en.wikipedia.org/wiki/Freedom_of_the_press
- https://en.wikipedia.org/wiki/Right_to_privacy
- https://en.wikipedia.org/wiki/Negative_liberty
- https://www.ftc.gov/sites/default/files/documents/public_comments/pr-eliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00298-57628.pdf
- https://en.wikipedia.org/wiki/Right_to_be_forgotten#Conception_and_proposal
- https://en.wikipedia.org/wiki/Letting_the_cat_out_of_the_bag
- <http://idioms.thefreedictionary.com/genie+back+in+the+bottle>
- <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>
- <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463256041805&uri=CELEX:31995L0046>
- <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11341>
- <http://tiny.cc/statecitizenship>
- https://en.wikipedia.org/wiki/Streisand_effect
- <http://www.thelastbastille.com/2014/04/26/administrative-agencies-the-fourth-branch-of-government/>
- <https://www.ftc.gov/about-ftc/biographies/julie-brill>
- https://www.ftc.gov/system/files/documents/public_statements/581751/140911mentorgroup.pdf
- <https://www.ftc.gov/public-statements/2015/04/why-you-have-right-obscurity>
- <http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/>

- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357
- <http://www.thelastbastille.com/2016/01/26/democracy-in-america/>
- <http://tiny.cc/skepticism>
- <http://www.thelastbastille.com/2014/07/09/i-pencil/>
- <http://www.thelastbastille.com/2015/06/27/we-dont-live-in-a-police-state/>
- <http://www.thelastbastille.com/2012/10/15/the-new-world-order/>
- <http://www.thelastbastille.com/2013/11/08/common-law-legally-defined/>
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2027018
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2473151
- http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2410240
- <http://tiny.cc/vetting>
- <https://fee.org/articles/mises-hayek-and-the-market-process-an-introduction/>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- <http://www.thelastbastille.com/2016/04/27/mark-dice-flip-flopping-truther-2012-2013/>
- <http://www.thelastbastille.com/2016/04/29/george-hemminger-just-prepper-character-2014/>
- <http://www.thelastbastille.com/2016/05/06/ron-paul-deserve-forgotten/>
- <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html>
- https://en.wikipedia.org/wiki/Historical_revisionism
- https://en.wikipedia.org/wiki/Historical_record
- https://youtu.be/ww_z6Teynow?t=3m37s
- <http://www.consumerwatchdog.org/resources/ltrpagertbf101314.pdf>
- https://en.wikipedia.org/wiki/Digital_footprint
- <https://myshadow.org/digital-traces-content-and-metadata>
- <http://www.thelastbastille.com/2016/05/01/charles-dyer-manhunt-2011/>
- <https://securityinabox.org/>
- <https://myshadow.org/>
- <http://www.libertyunderattack.com/solutions/>
- <https://arxiv.org/abs/1506.06033>
- <http://www.thelastbastille.com/2011/12/31/problem-reaction-solution-hegelian-dialectic/>
- https://en.wikipedia.org/wiki/Extraordinary_rendition
- https://en.wikipedia.org/wiki/Black_operations

- <https://youtu.be/PqLSs49fSds?t=30s>
- https://en.wikipedia.org/wiki/Creative_destruction
- <https://www.cnil.fr/fr/node/15790>
- <http://peterfleischer.blogspot.co.nz/2011/03/foggy-thinking-about-right-to-oblivion.html>
- <http://www.thelastbastille.com/2014/08/16/against-intellectual-property/>
- <https://en.wikipedia.org/wiki/Recidivism>
- <http://outpost-of-freedom.com/MasseyL12.htm>
- <http://www.thelastbastille.com/2012/05/10/evil-in-itself-or-just-forbidden/>
- <http://www.thelastbastille.com/2014/01/07/three-felonies-a-day/>
- https://en.wikipedia.org/wiki/Victimless_crime
- <https://tiny.cc/individuality>
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- <http://www.thelastbastille.com/2012/08/28/albions-seed/>
- <http://www.thelastbastille.com/2015/02/21/whos-watching-you/>

Sifting the Wheat from the Chaff: The Value of Skepticism

- https://en.wikipedia.org/wiki/The_Sign_of_the_Four
- <http://www.thelastbastille.com/2013/06/16/carousel-of-carnivores/>
- <http://christophercantwell.com/2015/01/24/7-steps-becoming-celebritarian/>
- <http://www.thelastbastille.com/2013/07/01/should-you-avoid-the-news/>
- <https://www.youtube.com/user/MatthewPatrick13/videos?view=0&flow=grid>
- <https://www.youtube.com/user/FilmTheorists/videos>
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- <https://youtu.be/ASODMKCJcsk?t=4m23s>
- <http://www.thelastbastille.com/2012/01/13/robert-steele-on-blogging/>
- https://en.wikipedia.org/wiki/Sophism#Modern_usage
- https://en.wikipedia.org/wiki/Razor_%28philosophy%29
- https://en.wikipedia.org/wiki/Hitchens%27s_razor
- https://en.wikipedia.org/wiki/Hanlon's_razor
- https://en.wikipedia.org/wiki/Occam's_razor

- <http://www.thelastbastille.com/2015/04/10/statist-fallacies/>
- https://en.wikipedia.org/wiki/Process_of_elimination
- <http://idioms.thefreedictionary.com/separate+the+wheat+from+the+chaff>
- <http://www.libertyunderattack.com/patriot-mythology-a-five-part-series/>
- <http://www.thelastbastille.com/2012/08/06/debating-does-not-work/>
- <http://www.infowars.com/u-s-postal-service-expands-construction-of-secret-rooms/>
- <http://www.thelastbastille.com/2014/02/03/only-on-paper-the-pathetic-story-of-commerical-redemption-freemen-on-the-land-sovereign-citizens-lawful-rebellion-community-immunity/>
- <https://en.wikipedia.org/wiki/Falsifiability>
- https://en.wikipedia.org/wiki/Oath_Keepers
- <https://www.oathkeepers.org/declaration-of-orders-we-will-not-obey/>
- <http://www.thelastbastille.com/2013/04/19/the-myth-of-the-line-in-the-sand/>
- http://www.outpost-of-freedom.com/radio/bel/131026_False_Hopes_Oathkeepers_Constitutional_Sheriffs_and_Filming_Cops.mp3
- <https://www.oathkeepers.org/about/>
- <http://www.heritage.org/constitution/articles/6/essays/134/oaths-clause>
- https://en.wikipedia.org/wiki/United_States_Armed_Forces_oath_of_enlistment
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title10/html/USCODE-2012-title10-subtitleA-partII-chap31-sec502.htm>
- <http://www.thelastbastille.com/2015/12/09/are-you-obligated-to-register-for-the-draft/>
- https://en.wikipedia.org/wiki/Oath_of_Allegiance_%28United_States%29#Text
- <https://www.gpo.gov/fdsys/pkg/CFR-2012-title8-vol1/pdf/CFR-2012-title8-vol1-sec337-1.pdf>
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>

- https://en.wikipedia.org/wiki/Scout_Promise#Boy_Scouts_of_America
- <https://youtu.be/4HkSAewoESg?t=29m23s>
- https://youtu.be/4s_pvufopzs
- <https://youtu.be/TUoOuayfOkM>
- <https://www.oathkeepers.org/ammon-bundy-martyr-or-revolutionary/>
- <http://www.libertyunderattack.com/citizens-for-constitutional-freedom/>
- https://en.wikipedia.org/wiki/3_Percenter
- <http://sipseystreetirregulars.blogspot.com/2009/02/what-is-three-percenter.html>
- <http://sipseystreetirregulars.blogspot.com/>
- <https://books.google.com/books?id=xK1NuzpAcH8C&pg=PA235>
- <http://oll.libertyfund.org/titles/adams-the-works-of-john-adams-vol-10-letters-1811-1825-indexes>
- <http://founders.archives.gov/documents/Adams/99-02-02-6140>
- <http://www.thelastbastille.com/2012/11/20/common-sense/>
- <http://founders.archives.gov/documents/Adams/99-02-02-6401>
- <https://en.wikipedia.org/wiki/Jacobin>
- <http://allthingsliberty.com/2013/02/john-adamss-rule-of-thirds/>
- <http://www.thelastbastille.com/2013/04/19/the-myth-of-the-line-in-the-sand/>
- <http://www.thelastbastille.com/2014/02/03/only-on-paper-the-pathetic-story-of-commerical-redemption-freemen-on-the-land-sovereign-citizens-lawful-rebellion-community-immunity/>
- <http://sipseystreetirregulars.blogspot.com/2010/02/yeah-but-what-does-that-three-percent.html>
- <http://sipseystreetirregulars.blogspot.com/2014/06/a-brief-three-percent-catechism.html>
- <http://www.thelastbastille.com/2012/02/23/leaderless-resistance-an-overview/>
- <http://www.threepcenter.org/read.php?4,8>
- <http://threepcenternation.com/f-a-q/>
- <http://threepcentersclub.org/index.php/pages/about-us>
- <http://sipseystreetirregulars.blogspot.com/2016/01/3-of-oregon-official-press-release.html>
- <http://www.iiipercentsidaho.org/>
- <http://www.thelastbastille.com/2013/04/16/protesting-does-not-work/>
- <https://youtu.be/CQo1x-pwozc?t=2m50s>
- <http://www.thelastbastille.com/2015/07/06/give-me-liberty/>

- https://en.wikipedia.org/wiki/Refugees_of_the_Syrian_Civil_War
- <http://www.thelastbastille.com/2016/02/27/the-neocon-infiltration-of-the-patriot-movement/>
- http://www.oregonlive.com/oregon-standoff/2016/01/brandon_curtiss_pacific_patrio.html
- <http://www.libertyunderattack.com/sean-anderson/>
- <http://www.thelastbastille.com/2016/02/08/sean-anderson-asks-where-the-three-percenters-fled-and-david-fry-joyrides-a-government-pickup-truck-video/>
- <http://www.thelastbastille.com/2016/01/20/operation-freedom-ride-video/>
- <http://outpost-of-freedom.com/blog/?p=1349>
- https://en.wikipedia.org/wiki/2015_Chattanooga_shootings
- <https://www.oathkeepers.org/oath-keepers-national-call-to-action-help-us-protect-the-protectors-by-guarding-recruiting-and-reserve-centers/>
- <http://www.military.com/daily-news/2015/07/22/army-to-recruiters-treat-armed-citizens-as-security-threat.html>
- <http://www.thelastbastille.com/2015/04/20/a-proposed-business-model-for-defending-texan-ranchers/>
- <http://www.thelastbastille.com/2016/02/24/mark-kessler-an-enemy-of-liberty/>
- <http://www.thelastbastille.com/2016/02/26/texas-constitutional-sheriff-letters-2013/>
- https://youtu.be/pj_3M_RvKVY?t=34m30s
- <http://www.statutes.legis.state.tx.us/Docs/SDocs/THETEXASCONSTITUTION.pdf>
- <http://www.thelastbastille.com/2013/05/02/should-you-resist-the-united-states-census/>
- <http://www.libertyunderattack.com/williamson-county-commissioners-court-meeting-9-29-15/>
- <http://outpost-of-freedom.com/blog/?p=1165>
- <https://youtu.be/iTj5Jw93Gyg>
- <http://www.thelastbastille.com/2014/09/19/stealing-your-life-away-the-threat-of-civil-asset-forfeiture/>
- <https://www.youtube.com/playlist?list=PLSFAEBtQDKZ6ePKc1kJVpwA2YwD5WRTLE>
- <http://www.thelastbastille.com/2016/02/28/anthony-bosworth-admits-he-is-a-failure/>
- <http://www.libertyunderattack.com/cancel-your-voter-registration/>

- <http://sos.state.tx.us/elections/candidates/guide/qualifications.shtml>
- <http://www.thelastbastille.com/2015/07/09/running-for-public-office-does-not-work-why-infiltrating-the-state-is-foolish/>
- <https://youtu.be/t4JeaYwdjTY>
- https://youtu.be/nKPp_DZM_Bk
- <http://www.thelastbastille.com/2016/01/29/are-benjamin-tuckers-four-monopolies-constitutional/>
- <http://www.cspoa.org/>
- <http://www.thelastbastille.com/2013/08/09/the-production-of-security/>
- <http://fprnradio.com/liberty-under-attack-121315/>
- <http://www.heritage.org/constitution/articles/1/essays/67/appropriations-clause>
- <http://www.thelastbastille.com/2012/11/15/ratification/>
- <http://www.thelastbastille.com/2013/06/23/the-federalist-papers/>
- <http://www.outpost-of-freedom.com/hh02a.htm>
- <http://www.thelastbastille.com/2015/06/29/grassroots-lobbying-does-not-work-a-review-of-chris-cantwells-anarcho-lobbyist-series-season-one/>
- <http://www.thelastbastille.com/2012/06/01/voting-does-not-work/>
- <http://www.thelastbastille.com/2014/09/12/jury-nullification-does-not-work/>
- <http://www.libertyunderattack.com/cancel-your-voter-registration/>
- <http://www.thelastbastille.com/downloadables/>
- <https://www.libertyclassroom.com/objections/>
- <http://fija.org/about/history/>
- <http://tracking.tenthamentcenter.com/>
- <http://tenthamentcenter.com/report/>
- <http://www.legis.state.tx.us/Resources/FAQ.aspx>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=HB21>
- <http://www.texasbulliondepository.com/>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=HB483>
- <http://www.opencarrytexas.org/the-law.html>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=HB910>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB642>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=83R&Bill=HB912>

- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=SB1286>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=HB2867>
- <http://www.thelastbastille.com/2015/03/19/education-free-compulsory/>
- <http://outpost-of-freedom.com/blog/?p=768>
- <https://youtu.be/mmyndl2NuFI>
- <http://www.thelastbastille.com/2013/01/10/the-probability-broach/>
- https://en.wikipedia.org/wiki/Historical_fiction
- <http://www.thelastbastille.com/2016/03/01/patrick-henrys-great-objection-constitution/>
- <http://www.thelastbastille.com/2015/07/13/coup-detat-a-practical-handbook/>
- <http://www.thelastbastille.com/2013/07/12/the-anti-federalist-papers/>
- [https://en.wikipedia.org/wiki/V_for_Vendetta_\(film\)](https://en.wikipedia.org/wiki/V_for_Vendetta_(film))
- <http://www.thelastbastille.com/2016/01/18/the-presidents-tailored-suit/>
- <http://freekeene.com/2012/11/15/your-vote-counts-in-nh-anarchist-wins-by-one-vote-in-manchester/>
- <http://www.thelastbastille.com/2014/07/12/super-stef/>
- <http://www.thelastbastille.com/2013/09/24/the-origins-of-war-in-child-abuse/>
- <http://www.thelastbastille.com/2014/02/13/beating-the-devil-out-of-them/>
- <http://www.thelastbastille.com/2014/02/22/hold-on-to-your-kids/>
- <http://www.thelastbastille.com/2014/02/13/beating-the-devil-out-of-them/>
- <http://www.thelastbastille.com/2013/09/10/no-treason-vi-the-constitution-of-no-authority/>
- <http://www.thelastbastille.com/2014/04/26/administrative-agencies-the-fourth-branch-of-government/>
- <http://www.thelastbastille.com/2014/02/13/beating-the-devil-out-of-them/>
- <https://youtu.be/sEAZ-BMbshw>
- <http://www.thelastbastille.com/2012/02/24/the-last-bastille-podcast-43-philosophy/>
- <http://www.thelastbastille.com/2015/11/13/neither-bullets-nor-ballots/>
- <http://www.thelastbastille.com/2015/05/05/freedom/>
- [https://en.wikipedia.org/wiki/Non_sequitur_\(logic\)](https://en.wikipedia.org/wiki/Non_sequitur_(logic))

- <http://www.thelastbastille.com/2016/02/25/you-are-known-by-the-company-you-keep-how-to-choose-your-allies-wisely/>
- https://en.wikipedia.org/wiki/Lenore_Skenazy
- <http://www.freerangekids.com/faq/>
- <https://youtu.be/DcrfuIEbfpA?t=23m01s>
- https://en.wikipedia.org/wiki/Tilting_at_windmills
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- <http://www.libertyunderattack.com/the-freedom-umbrella-of-direct-action-second-edition/>
- <http://www.thelastbastille.com/2014/02/26/the-politics-of-obedience/>
- <http://www.thelastbastille.com/2013/06/11/the-society-of-the-spectacle/>
- <http://www.thelastbastille.com/2012/11/14/conspiratainment/>
- <http://www.thelastbastille.com/2012/08/25/blogosphere/>
- <https://youtu.be/J6qT6Nwj0OU>
- <https://youtu.be/RrjPLgyVIBc>
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- <http://www.libertyunderattack.com/court-documents/>
- <http://www.thelastbastille.com/2014/07/17/economics-in-one-lesson/>
- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>

Modeling Threats & Analyzing Risks: A Rebuttal Against “Doom Porn”

- https://en.wikipedia.org/wiki/Jeremiah_%28TV_series%29
- https://en.wikipedia.org/wiki/Jericho_%282006_TV_series%29
- https://en.wikipedia.org/wiki/The_Walking_Dead_%28franchise%29
- <http://www.tedxpsu.com/about-2/about-tedxpsu/>
- http://www.ted.com/talks/bruce_schneier/transcript?language=en
- https://en.wikipedia.org/wiki/Confirmation_bias
- https://en.wikipedia.org/wiki/Normalcy_bias
- <http://www.thelastbastille.com/2013/07/01/should-you-avoid-the-news/>
- <http://www.thelastbastille.com/2014/07/17/economics-in-one-lesson/>
- <http://www.thelastbastille.com/2012/06/22/is-substance-abuse-the-same-as-addiction/>

- <http://www.thelastbastille.com/2012/10/16/victim-mentality>
- https://en.wikipedia.org/wiki/New_media
- https://en.wikipedia.org/wiki/Availability_heuristic
- <https://www.youtube.com/user/TheLordHumungus/videos>
- https://youtu.be/SlhM_8TtvZ0
- <https://youtu.be/f-F-80K2chk>
- <https://youtu.be/WPdWg8YtL44>
- <https://tinyurl.com/chillingdissent>
- <https://en.wikipedia.org/wiki/Precognition>
- <https://ssd.eff.org/en/glossary/threat-model>
- <https://ssd.eff.org/en/glossary/risk-analysis>
- <http://doomporn.com/blog>
- <http://www.urbandictionary.com/define.php?term=doom+porn>
- <http://www.thelastbastille.com/2013/10/26/the-anti-terrorist-handbook/>
- <http://www.9-11commission.gov/report/911Report.pdf>
- http://www.ct.gov/csao/lib/csao/Sandy_Hook_Final_Report.pdf
- <https://en.wikipedia.org/wiki/Credulity>
- <https://tinyurl.com/homeschoolingprimer>
- <http://www.newyorker.com/magazine/2015/07/20/the-really-big-one>
- <https://youtu.be/sTx-3Sxc1k4>
- <https://www.thestranger.com/blogs/slog/2015/07/14/22540273/the-five-scariest-takeaways-from-the-new-yorker-article-about-the-earthquake-that-will-devastate-seattle>
- http://www.slate.com/articles/health_and_science/science/2015/07/kathryn_schulz_s_new_yorker_story_on_pacific_northwest_earthquake_geologists.html
- https://www.reddit.com/r/IAmA/comments/3da1mh/we_are_earthquake_experts_ask_us_anything_about/ct36evt
- https://www.reddit.com/r/IAmA/comments/3da1mh/we_are_earthquake_experts_ask_us_anything_about/ct373sk
- <http://www.thelastbastille.com/2012/07/13/controlled-opposition/>
- <http://geosociety.org/gsatoday/archive/25/8/article/i1052-5173-25-8-4.htm>
- <http://www.sciencedaily.com/releases/2015/07/150728101212.htm>
- <http://www.thelastbastille.com/2015/05/05/freedom/>
- https://en.wikipedia.org/wiki/Weather_warfare
- <https://youtu.be/u-sRbR2QQ7w>
- <http://www.thelastbastille.com/2011/12/31/problem-reaction-solution-hegelian-dialectic/>

- <http://www.thelastbastille.com/2012/08/11/the-internet/>
- <http://www.zerohedge.com/>
- <http://trendsresearch.com/trends-journal/>
- <http://theeconomiccollapseblog.com/>
- <https://youtu.be/jcAi0ZUDVgo>
- https://en.wikipedia.org/wiki/Mad_Max_2
- https://api.soundcloud.com/tracks/218314889/download?secret_token=s-sgU1D&client_id=0f8fdbbaa21a9bd18210986a7dc2d72c
- https://en.wikipedia.org/wiki/Dow_Jones_Industrial_Average
- <https://en.wikipedia.org/wiki/DAX>
- https://en.wikipedia.org/wiki/Shanghai_Stock_Exchange
- https://en.wikipedia.org/wiki/Nikkei_225
- <https://www.lewrockwell.com/2010/05/stewart-dougherty/the-dollar-rally-is-hugely-bullish-for-preciousmetals/>
- https://en.wikipedia.org/wiki/Austrian_business_cycle_theory
- <https://www.youtube.com/user/BrotherJohnF/videos>
- <https://www.youtube.com/user/SGTbull07/videos>
- <https://www.youtube.com/user/TruthNeverTold/videos>
- <http://silver-stacking.com/news/about-us/>
- <http://www.futuresmag.com/2015/05/01/jpmorgan-chase-cornering-silver-bullion-market>
- <https://www.youtube.com/playlist?list=PL6bkc1Tz5QeQEltLADrZXvID8K7Cr9rZP>
- <http://www.thelastbastille.com/2012/02/13/fake-awake/>
- <http://www.thelastbastille.com/2012/10/04/fractional-reserve-lending/>
- https://en.wikipedia.org/wiki/The_Goose_That_Laid_the_Golden_Eggs
- https://en.wikipedia.org/wiki/1998%E2%80%932002_Argentine_great_depression
- https://en.wikipedia.org/wiki/Hyperinflation_in_Zimbabwe
- https://en.wikipedia.org/wiki/Bank_of_England
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- <https://youtu.be/UI7K2yXMucE>
- <https://en.wikipedia.org/wiki/Hyperinflation>
- [https://en.wikipedia.org/wiki/Depression_\(economics\)](https://en.wikipedia.org/wiki/Depression_(economics))
- https://en.wikipedia.org/wiki/Currency_war
- https://youtu.be/wy5Bw_7jgds
- https://en.wikipedia.org/wiki/Government_failure
- <http://www.federalreserve.gov/monetarypolicy/fomcminutes20150729.htm>

- <https://en.wikipedia.org/wiki/Malinvestment>
- https://en.wikipedia.org/wiki/Hyperinflation#Hyperinflationary_episodes
- http://survivalus.blogspot.com/2010/11/hyperinflation-in-american-civil-war_29.html
- https://en.wikipedia.org/wiki/United_States#History
- <https://thelastbastille.wordpress.com/2014/07/09/i-pencil/>
- <https://thelastbastille.wordpress.com/2013/02/17/warfare-state/>
- https://youtu.be/8MxVuSnW_6A
- https://en.wikipedia.org/wiki/Revolution_%28TV_series%29
- https://en.wikipedia.org/wiki/Solar_storm_of_1859
- <http://www-istp.gsfc.nasa.gov/istp/nicky/cme-chase.html>
- https://en.wikipedia.org/wiki/North_American_Electric_Reliability_Corporation
- <http://www.balch.com/files/upload/2012NERCGMDReport.pdf>
- <http://energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf>
- https://en.wikipedia.org/wiki/Precautionary_principle
- https://en.wikipedia.org/wiki/Federal_Energy_Regulatory_Commission
- <https://tinyurl.com/fourthbranchofgovernment>
- <http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf>
- <http://www.gpo.gov/fdsys/pkg/STATUTE-119/pdf/STATUTE-119-Pg594.pdf>
- <http://www.ferc.gov/CalendarFiles/20120502132652-Pry,%20Homeland%20Security.pdf>
- https://en.wikipedia.org/wiki/One_Second_After
- <http://www.dod.mil/dodgc/olc/docs/2001NDAA.pdf>
- <http://empcommission.org/>
- <http://empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf>
- <https://tinyurl.com/dragnetwiretapping>
- <https://youtu.be/lA9KaeyFEMc?t=1m33s>
- <https://youtu.be/vn6OVLK0MBI>
- https://en.wikipedia.org/wiki/Texas_Interconnection
- <https://en.wikipedia.org/wiki/Rulemaking>
- <https://youtu.be/MFKApB23fnA>

- <http://www.nap.edu/catalog/12507/severe-space-weather-events-understanding-societal-and-economic-impacts-a>
- http://www.nist.gov/customcf/get_pdf.cfm?pub_id=861610
- https://en.wikipedia.org/wiki/National_Oceanic_and_Atmospheric_Administration
- <http://www.inquisitr.com/1121454/solar-flares-noaa-says-80-percent-chance-of-earth-directed-eruptions-today/>
- https://www.nasa.gov/mission_pages/sunearth/news/News051213-flare.html
- <http://www.wired.com/2012/02/massive-solar-flare/>
- http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/
- https://en.wikipedia.org/wiki/Earth's_orbit
- <http://www.thelastbastille.com/2013/12/18/hyperspace/>
- <https://youtu.be/FW8Rsil0lqk>
- <http://tinyurl.com/grassrootslobbying>
- <http://history1900s.about.com/od/worldwarii/a/hiroshima.htm>
- https://en.wikipedia.org/wiki/Mutual_assured_destruction
- https://en.wikipedia.org/wiki/Nuclear_holocaust
- <http://libertariangaming.org/2015/08/29/hurricane-katrina-ten-years-after-trusting-the-government-went-really-bad/>
- <https://youtu.be/Klqv9t1zVww?t=17m13s>
- <https://youtu.be/VebOTc-7shU?t=46m20s>
- https://en.wikipedia.org/wiki/Pre-emptive_nuclear_strike
- <https://youtu.be/HP7L8bw5QF4>
- <http://www.outpost-of-freedom.com/factions.htm>
- <http://www.centerforsecuritypolicy.org/upload/wysiwyg/article%20pdfs/Shariah%20-%20The%20Threat%20to%20America%20%28Team%20B%20Report%29%20Web%20Version%2009302010.pdf>
- <http://www.actforamerica.org/about-brigitte-gabriel>
- https://en.wikipedia.org/wiki/Curtis_Culwell_Center_attack
- https://en.wikipedia.org/wiki/2015_Chattanooga_shootings
- <https://youtu.be/K7aFXRAW7mg?t=1m34s>
- <https://en.wikipedia.org/wiki/Islamism>
- <http://www.libertyunderattack.com/terror-industrial-complex-timeline/>
- https://en.wikipedia.org/wiki/Operation_Cyclone
- <https://en.wikipedia.org/wiki/Al-Qaeda>
- https://en.wikipedia.org/wiki/Blowback_%28intelligence%29

- <http://www.pbs.org/wgbh/pages/frontline/rise-of-isis/>
- http://original.antiwar.com/Dan_Sanchez/2015/06/08/the-us-governments-not-so-secret-support-for-al-qaeda-and-isis/
- <https://tinyurl.com/chillingdissent>
- https://en.wikipedia.org/wiki/William_Kristol
- https://en.wikipedia.org/wiki/Coptic_Orthodox_Church_of_Alexandria
- <http://outpost-of-freedom.com/blog/?p=906>
- <https://thelastbastille.wordpress.com/2014/01/24/thomas-jefferson-built-a-wall-of-separation-between-church-state/>
- <https://en.wikipedia.org/wiki/Islamism>
- https://upload.wikimedia.org/wikipedia/commons/8/82/Article_11.gif
- https://en.wikipedia.org/wiki/Thomas_Browne
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- https://en.wikipedia.org/wiki/Baton_%28law_enforcement%29
- <https://reason.com/archives/2011/07/18/fear-of-a-muslim-america/1>
- <http://www.thelastbastille.com/2012/07/26/islam-is-not-the-problem/>
- <https://tinyurl.com/chillingdissent>
- https://en.wikipedia.org/wiki/Clarion_Project
- https://en.wikipedia.org/wiki/Raphael_Shore
- https://youtu.be/9RC1Mepk_Sw
- <https://www.youtube.com/user/maryamrajavi/videos>
- <http://www.ncr-iran.org/en/>
- <https://en.wikipedia.org/wiki/Madrasa>
- <https://tinyurl.com/homeschoolingprimer>
- <http://www.loonwatch.com/2012/06/most-victims-of-islamic-terrorism-are-muslims-and-why-america-is-to-blame-for-it/>
- <http://www.middleeasteye.net/columns/unworthy-victims-western-wars-have-killed-four-million-muslims-1990-39149394>
- <https://en.wikipedia.org/wiki/Islamization>
- https://upload.wikimedia.org/wikipedia/commons/b/ba/Islam_percent_population_in_each_nation_World_Map_Muslim_data_by_Pew_Research.svg
- http://www.answers.com/Q/How_many_Christians_are_there_in_the_US
- <https://tinyurl.com/defendingtexanranchers>
- http://www.dispatch.com/content/stories/local/2015/07/20/guarding_recruitment_centers.html
- https://en.wikipedia.org/wiki/Posse_Comitatus_Act
- <https://youtu.be/FjZVLHPV7wA>

- <http://www.thelastbastille.com/2013/07/01/should-you-avoid-the-news/>
- <http://www.libertyunderattack.com/ettw-qa/>
- <http://www.libertyunderattack.com/the-communist-state-of-illinois-voting-does-not-work-an-analysis/>
- <http://www.skepticsannotatedbible.com/1cor/13.html>
- <https://en.wikipedia.org/wiki/Rapture>
- https://en.wikipedia.org/wiki/2011_end_times_prediction
- <https://youtu.be/f9KlMWzKj4s>
- <https://youtu.be/7BJ9U4iZcxk>
- https://en.wikipedia.org/wiki/End_time
- https://en.wikipedia.org/wiki/Great_Tribulation
- <https://en.wikipedia.org/wiki/Antichrist>
- <https://en.wikipedia.org/wiki/Jesus>
- https://en.wikipedia.org/wiki/Islamic_eschatology
- <https://en.wikipedia.org/wiki/Mahdi>
- https://en.wikipedia.org/wiki/Masih_ad-Dajjal
- https://en.wikipedia.org/wiki/Last_Judgment
- https://en.wikipedia.org/wiki/Conceptions_of_God
- <https://en.wikipedia.org/wiki/Irreligion>
- <http://www.thelastbastille.com/2015/08/05/the-conscious-resistance/>
- <https://thelastbastille.wordpress.com/2012/01/06/religion/>
- http://www.deism.com/deism_defined.htm
- https://en.wikipedia.org/wiki/Confidence_trick
- https://youtu.be/qIAwYLOXV_I
- https://en.wikipedia.org/wiki/Triune_brain#Reptilian_complex
- https://en.wikipedia.org/wiki/Lifeboat_ethics
- <http://dailyanarchist.com/2013/01/09/expanding-on-rothbards-lifeboat-situations/>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- <http://www.donotlink.com/gizq>
- https://en.wikipedia.org/wiki/Tabletop_game
- <http://www.thelastbastille.com/2012/09/13/vetting/>
- http://traffic.libsyn.com/survivalistprepper/SPP021_Conflicted_The_Game.mp3
- <https://youtu.be/tLXP6ozEqqs>
- https://en.wikipedia.org/wiki/Hard_cases_make_bad_law
- <http://www.thelastbastille.com/2013/04/19/the-myth-of-the-line-in-the-sand/>
- https://en.wikipedia.org/wiki/Non_sequitur_%28logic%29

- <https://tinyurl.com/homeschoolingprimer>
- <http://survivalblog.com/glossary/g/#G.O.O.D.>
- <http://www.internetarmory.com/>
- <http://www.libertyunderattack.com/cancel-your-voter-registration/>
- https://en.wikipedia.org/wiki/Government_monopoly
- <http://www.thelastbastille.com/2014/07/09/i-pencil/>
- https://en.wikipedia.org/wiki/Government_failure
- <http://www.libertyunderattack.com/lu-radio-the-united-police-states-of-america/>
- <https://tinyurl.com/civilassetforfeiture>
- <https://tinyurl.com/dragnetwiretapping>
- <http://www.thelastbastille.com/2013/03/23/death-by-government/>
- <http://www.thelastbastille.com/2015/06/27/we-dont-live-in-a-police-state/>
- <http://gizmodo.com/5524843/police-seize-jason-chens-computers>
- <http://www.avoiceformen.com/mens-rights/texas-legislates-against-paternity-fraud/>
- <https://tinyurl.com/chillingdissent>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- http://www.therebel.media/why_i_am_not_a_feminist
- <http://aaamath.com/rat62b-findratios.html>
- https://en.wikipedia.org/wiki/Middle_school
- <https://tinyurl.com/homeschoolingprimer>
- <http://www.thelastbastille.com/2013/02/26/travel-trailer-homesteading-under-5000/>
- <http://www.thelastbastille.com/2013/09/02/the-activist-legal-defense-fund-scam/>
- <http://www.libertyunderattack.com/solutions/>
- https://en.wikipedia.org/wiki/Institutional_analysis
- <http://www.libertyunderattack.com/reformism-does-not-work-a-critique-of-political-activism/>
- <http://www.thelastbastille.com/2013/08/23/a-revelation-of-the-method/>
- <http://www.thelastbastille.com/2012/10/16/victim-mentality/>
- https://en.wikipedia.org/wiki/Live_action_role-playing_game
- https://24.media.tumblr.com/tumblr_mdX5ctzdDg1rl07u1o1_1280.jpg
- <http://www.libertyunderattack.com/the-freedom-umbrella-of-direct-action/>
- <https://soundcloud.com/magnum71/r-e-m-its-the-end-of-the-world>

The Libertarian Case for Judicial Transparency

- http://www.constitution.org/lrev/rodell/woe_onto_you_lawyers.htm
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>
- <http://www.thelastbastille.com/2016/01/29/are-benjamin-tuckers-four-monopolies-constitutional/>
- <http://www.thelastbastille.com/2014/05/24/woe-onto-you-lawyers/>
- https://en.wikipedia.org/wiki/Police_perjury
- https://en.wikipedia.org/wiki/Modus_operandi
- <http://www.libertyunderattack.com/>
- <http://www.libertyunderattack.com/court-documents/>
- <http://www.thelastbastille.com/>
- <http://www.libertyunderattack.com/wp-content/uploads/Documents/Anthology%20-%20Adventures%20in%20Illinois%20Law.pdf>
- <http://www.libertyunderattack.com/charles-dyers-court-documents/>
- <http://www.thelastbastille.com/2015/07/14/suing-the-government-does-not-work-lawsuits-are-not-useful-for-securing-your-liberty/>
- <http://www.libertyunderattack.com/stonewalled-there-is-no-hope-for-charles-dyer/>
- <https://youtu.be/cpcFQrSbxzc>
- <http://bundryranch.blogspot.com/2015/11/facts-events-in-hammond-case.html>
- <http://www.libertyunderattack.com/ammon-bundy/>
- <https://www.youtube.com/playlist?list=PLtPAcvJ-f939x493pSkz61M5TikyHsXQT>
- <https://youtu.be/U1BCMjIV83E?t=5m37s>
- <https://youtu.be/5VIn7IemKTE>
- <http://thepetesantillishow.com/hammond-legal-file/>
- <http://www.libertyunderattack.com/wp-content/uploads/Documents/--Hammond%20Legal%20Files--.pdf>
- <https://www.youtube.com/watch?v=WxaNHJ1rLxo&list=PLtPAcvJ-f93-VO3JroizIEOG4d3txwwV6&index=18>
- [https://en.wikipedia.org/wiki/Color_\(law\)](https://en.wikipedia.org/wiki/Color_(law))
- <https://www.youtube.com/watch?v=XeerCjYxaZU&list=PLtPAcvJ-f93-VO3JroizIEOG4d3txwwV6&index=30>
- <http://www.libertyunderattack.com/solutions/>
- <http://www.supremecourt.gov/opinions/opinions.aspx>

- <http://www.supremecourt.gov/opinions/boundvolumes.aspx>
- <http://openjurist.org/us>
- <https://www.law.cornell.edu/>
- <https://en.wikipedia.org/wiki/Paywall>
- <https://www.pacer.gov/psc/hfaq.html>
- <https://en.wikipedia.org/wiki/Hacktivism>
- <https://public.resource.org/about/index.html>
- https://en.wikipedia.org/wiki/Aaron_Swartz#PACER
- <http://www.search.txcourts.gov/CaseSearch.aspx?coa=cossup&s=c>
- <http://www.search.txcourts.gov/Case.aspx?cn=13-0006&coa=cossup>
- <http://www.thelastbastille.com/2014/09/19/stealing-your-life-away-the-threat-of-civil-asset-forfeiture/>
- <http://www.search.txcourts.gov/SearchMedia.aspx?MediaVersionID=5be576ce-9deb-409a-a595-310d66127842&coa=cossup&DT=OTHER&MediaID=4da82165-384f-4f28-bcb1-5bb051999a06>
- <https://tinyurl.com/politicalfieldtrips>
- <http://judicialrecords.wilco.org/default.aspx>
- <https://www.austintexas.gov/AmcPublicInquiry/pubportal.aspx?ReturnUrl=%2fAmcPublicInquiry%2fsearch%2fDocketSearch.aspx>
- [https://en.wikipedia.org/wiki/Docket_\(court\)](https://en.wikipedia.org/wiki/Docket_(court))
- <http://www.libertyunderattack.com/court-documents/>
- <http://www.libertyunderattack.com/wp-content/uploads/2015/06/150417-indictment-United-States-v.-William-Wolf.pdf>
- <http://www.donotlink.com/ep4t>
- https://en.wikipedia.org/wiki/Video_blog
- https://en.wikipedia.org/wiki/URL_shortening
- <http://www.thelastbastille.com/2013/09/02/the-activist-legal-defense-fund-scam/>
- <http://www.thelastbastille.com/2013/05/11/petitioning-does-not-work/>
- <http://www.foia.gov/about.html>
- <http://www.thelastbastille.com/2014/01/03/ian-bernard-the-man-who-snitched-on-larken-rose/>
- <http://freekeene.com/>
- <https://www.youtube.com/user/FreeKeene/videos>
- <https://thestanglx.wordpress.com/2014/05/04/free-keene-video-archival-court-footage-2008-2014/>
- https://en.wikipedia.org/wiki/Open-source_intelligence

Secured Record Archival: How to Protect Your Documents from the Government

- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>
- https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos
- https://en.wikipedia.org/wiki/Ashley_Madison_data_breach
- <http://www.thelastbastille.com/2016/06/14/vonu-search-personal-freedom/>
- <https://en.wikipedia.org/wiki/Originalism>
- https://en.wikipedia.org/wiki/Constitutional_law
- <http://tiny.cc/statecitizenship>
- [https://en.wikipedia.org/wiki/Color_\(law\)](https://en.wikipedia.org/wiki/Color_(law))
- <https://en.wikipedia.org/wiki/Lawfare>
- https://en.wikipedia.org/wiki/Defensive_computing
- <http://tiny.cc/leaderlessresistance>
- <https://en.wikipedia.org/wiki/Digitizing>
- <http://www.libertyunderattack.com/security-culture/>
- <http://www.thelastbastille.com/2016/06/22/home-hardening-fortify-domicile-intruders/>
- https://en.wikipedia.org/wiki/Information_technology_security_audit
- <http://tinyurl.com/cellphoneliberty>
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>
- <http://www.heritage.org/constitution/amendments/4/searches-and-seizures>
- https://en.wikipedia.org/wiki/Original_intent
- <http://www.thelastbastille.com/2013/07/12/the-anti-federalist-papers/>
- <http://www.thelastbastille.com/2012/11/15/ratification/>
- <http://www.heritage.org/constitution/articles/6/essays/133/supremacy-clause>
- https://en.wikipedia.org/wiki/Writ_of_assistance
- <https://1828.mshaffer.com/d/word/particular>
- <https://1828.mshaffer.com/d/word/describe>
- <https://tiny.cc/socialistinsecurity>
- <http://www.heritage.org/constitution/amendments/4/essays/145/warrant-clause>
- https://en.wikipedia.org/wiki/Searches_incident_to_a_lawful_arrest
- https://en.wikipedia.org/wiki/Motion_in_United_States_law
- https://en.wikipedia.org/wiki/Terry_stop

- <http://tiny.cc/dragnetwiretapping>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title42/html/USCODE-2013-title42-chap7-subchapII-sec405.htm>
- https://en.wikipedia.org/wiki/Exclusionary_rule
- https://en.wikipedia.org/wiki/Fruit_of_the_poisonous_tree
- <http://openjurist.org/392/us/1>
- <http://openjurist.org/395/us/752>
- <http://openjurist.org/414/us/218>
- <http://openjurist.org/995/f2d/776>
- <https://www.gpo.gov/fdsys/pkg/USCOURTS-ca7-10-03803/pdf/USCOURTS-ca7-10-03803-1.pdf>
- <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf>
- <http://www.libertyunderattack.com/wp-content/uploads/2015/06/140604-Indictment-United-States-v.-Robert-Beecher.pdf>
- <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/html/USCODE-2012-title18-partI-chap44-sec922.htm>
- http://www.libertyunderattack.com/wp-content/uploads/Documents/Beecher_Warrant.jpg
- <http://www.libertyunderattack.com/wp-content/uploads/2015/06/150402-Plea-Agreement-United-States-v.-Robert-Beecher.pdf>
- <http://www.libertyunderattack.com/schuyler-barbeau-2/>
- <http://www.libertyunderattack.com/wp-content/uploads/Documents/151216%20-%20Indictment.pdf>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title26/html/USCODE-2012-title26-subtitleE-chap53-subchapC-sec5861.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title26/html/USCODE-2012-title26-subtitleE-chap53-subchapB-partI-sec5845.htm>
- [http://www.libertyunderattack.com/wp-content/uploads/Documents/160225%20-%20Superseding%20Indictment%20\(United%20States%20v.%20Schuyler%20Barbeau\).pdf](http://www.libertyunderattack.com/wp-content/uploads/Documents/160225%20-%20Superseding%20Indictment%20(United%20States%20v.%20Schuyler%20Barbeau).pdf)
- <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/html/USCODE-2012-title18-partI-chap44-sec922.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/html/USCODE-2012-title18-partI-chap44-sec924.htm>

- <http://www.libertyunderattack.com/wp-content/uploads/Documents/151205%20-%20Search%20and%20Seizure%20Warrant.pdf>
- <http://codes.ohio.gov/orc/3717.21>
- http://blog.cleveland.com/metro/2008/12/_1209165828_001.pdf
- https://en.wikipedia.org/wiki/Tenth_Amendment_to_the_United_States_Constitution
- <https://www.legislature.ohio.gov/laws/ohio-constitution>
- <https://www.supremecourt.ohio.gov/rod/docs/pdf/9/2011/2011-ohio-2710.pdf>
- <http://farmtoconsumer.org/news/news-15dec2008-2.htm>
- <http://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf>
- https://en.wikipedia.org/wiki/Scholarly_peer_review
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <https://tinyurl.com/vonurayo>
- <http://minimalistpackrat.com/2011/09/19/a-minimalist-take-on-papers/>
- <http://www.missminimalist.com/2012/05/my-minimalist-filing-system/>
- <http://www.everydayminimalist.com/?p=179>
- <http://exilelifestyle.com/minimalism-explained/>
- <http://www.theminimalists.com/sentimental/>
- https://en.wikipedia.org/wiki/Filename_extension
- https://en.wikipedia.org/wiki/File_system#OS_X
- https://en.wikipedia.org/wiki/Computer_file
- <http://www.thelastbastille.com/2012/06/29/revamped-american-redoubt-prioritized-task-list/>
- <http://bemorewithless.com/the-possibility-of-paperless/>
- <http://www.backwoodshome.com/it-came-from-the-junk-drawer/>
- <http://tiny.cc/configurepgp4mac>
- <https://en.wikipedia.org/wiki/PunchedPocket>
- https://en.wikipedia.org/wiki/Filing_cabinet
- <https://youtu.be/hllGJZ40MbM>
- <https://youtu.be/wpIJVWXsBBI>
- <https://youtu.be/UhNvC38C2FU>
- <https://youtu.be/Pxlq7c5-tbw>
- <http://cdn.thisiswhyimbroke.com/images/compact-key-holder.jpg>
- https://en.wikipedia.org/wiki/Computational_hardness_assumption
- https://en.wikipedia.org/wiki/Key_size

- <https://diceware.blogspot.com/2013/12/making-random-letter-passwords-memorable.html>
- http://www.jbonneau.com/doc/BS12-USEC-passphrase_linguistics.pdf
- <http://world.std.com/~reinhold/diceware.html>
- <https://youtu.be/doGzuOYCNJE?t=37m59s>
- <https://youtu.be/JDaicPIgn9U>
- <https://youtu.be/Gi-niOoVAm4>
- https://en.wikipedia.org/wiki/User_error
- https://en.wikipedia.org/wiki/Password_manager
- https://en.wikipedia.org/wiki/Kensington_Security_Slot
- https://youtu.be/r84ue_aEkX0
- <https://en.wikipedia.org/wiki/Diaper>
- https://en.wikipedia.org/wiki/Thread_seal_tape
- <https://en.wikipedia.org/wiki/Desiccant>
- <https://en.wikipedia.org/wiki/Sachet>
- <http://lifehacker.com/269427/dry-out-your-soaked-gadgets-in-rice>
- <https://youtu.be/P5vkwiBykzc>
- https://youtu.be/nKPp_DZM_Bk
- https://en.wikipedia.org/wiki/Free_and_open-source_software
- https://en.wikipedia.org/wiki/Open-source_hardware
- <https://ssd.eff.org/>
- <https://securityinabox.org/>
- <http://www.thesafemac.com/>
- <https://prism-break.org/en/>
- <http://www.backwoodshome.com/it-came-from-the-junk-drawer/>
- <https://en.wikipedia.org/wiki/MacBook>
- https://en.wikipedia.org/wiki/Mac_OS_X_Snow_Leopard
- https://en.wikipedia.org/wiki/Avast_Software
- https://en.wikipedia.org/wiki/Clam_AntiVirus#Mac_OS_X
- <https://sqwarq.com/detectx/>
- https://en.wikipedia.org/wiki/Disk_Utility
- https://youtu.be/M6E4Xk5o0_c
- <https://en.wikipedia.org/wiki/Digitizing>
- https://en.wikipedia.org/wiki/Image_scanning
- [https://en.wikipedia.org/wiki/Preview_\(Mac_OS\)](https://en.wikipedia.org/wiki/Preview_(Mac_OS))
- [https://en.wikipedia.org/wiki/Finder_\(software\)](https://en.wikipedia.org/wiki/Finder_(software))
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- https://en.wikipedia.org/wiki/Microsoft_Word

- https://en.wikipedia.org/wiki/Microsoft_Excel
- https://en.wikipedia.org/wiki/USB_flash_drive
- https://en.wikipedia.org/wiki/Hard_disk_drive#External_hard_disk_drives
- https://en.wikipedia.org/wiki/OS_X_El_Capitan
- <http://www.cnet.com/news/os-x-disk-utility-missing-options-to-erase-free-disk-space/>
- <https://www.nsa.gov/resources/everyone/media-destruction/>
- <http://osxdaily.com/2015/10/12/secure-empty-trash-equivalent-mac-os-x/>
- <https://en.wikipedia.org/wiki/CD-R>
- https://en.wikipedia.org/wiki/DVD_recordable
- <https://en.wikipedia.org/wiki/CD-RW>
- https://en.wikipedia.org/wiki/Optical_disc
- https://www.schneier.com/blog/archives/2005/06/write_down_your.html
- http://www.urbachletter.com/Archive/Tech_1204_Diceware.htm
- <https://en.wikipedia.org/wiki/Dice>
- <http://www.urbachletter.com/1204/DicewareWordList.pdf>
- https://en.wikipedia.org/wiki/Rote_learning
- https://en.wikipedia.org/wiki/Password_manager
- <https://en.wikipedia.org/wiki/KeePassX>
- <http://www.cnet.com/news/securing-data-on-any-medium-in-os-x/>
- <https://en.wikipedia.org/wiki/GPGTools>
- <http://tiny.cc/configurepgp4mac>
- <http://www.thelastbastille.com/2016/05/22/dual-layer-encryption-proposal-sidestepping-potential-backdoors/>
- https://en.wikipedia.org/wiki/Cloud_computing
- <http://www.thelastbastille.com/2012/11/27/how-to-hide-anything/>
- <http://www.thelastbastille.com/2012/11/29/the-big-book-of-secret-hiding-places/>
- <http://www.thelastbastille.com/2012/12/03/how-to-hide-things-in-public-places/>
- <http://www.thelastbastille.com/2013/09/16/story-of-a-secret-state/>
- https://en.wikipedia.org/wiki/Address_book#Little_black_book
- https://en.wikipedia.org/wiki/Zipper_storage_bag
- <http://tiny.cc/doomporn>
- <http://ahistoryofviolenceinchicago.blogspot.com/2014/04/police-turn-to-al-capone-method-to-trap.html>
- https://en.wikipedia.org/wiki/Procedural_law

- https://en.wikipedia.org/wiki/Moore's_law
- https://en.wikipedia.org/wiki/Crypto_Wars
- <http://tiny.cc/dragnetwiretapping>
- <https://www.wired.com/2013/12/nsa-hacking-catalogue/>
- https://en.wikipedia.org/wiki/Black_hat
- https://en.wikipedia.org/wiki/Information_technology_security_audit
- <http://www.anagram.com/berson/abskyeval.html>
- <http://www.thesafemac.com/mac-anti-virus-testing-2014/>
- <https://eprint.iacr.org/2012/374>
- <https://defuse.ca/audits/encfs.htm>
- <https://en.wikipedia.org/wiki/EncFS>
- <https://opencryptoaudit.org/>
- <https://en.wikipedia.org/wiki/TrueCrypt>
- <https://prism-break.org/en/>
- <https://zomiaofflinegames.com/darkandroid/>
- <https://sourceforge.net/p/keepass/discussion/329220/thread/0297bf6d/>
- <https://gpgtools.org/opensource.html>
- <http://www.getsafe.org/about#securityaudit>
- <https://spideroak.com/articles/responsibly-bringing-a-new-cryptography-product-to-market>
- <https://crypton.io/docs/security/audits.html>
- <https://www.gofundme.com/PulseVictimsFund>
- <https://youtu.be/52AaT9IO6QU>
- <https://youtu.be/XeerCjYxaZU>
- <http://www.thelastbastille.com/tax-ban-or-regulate/>
- <http://www.thelastbastille.com/2016/06/22/home-hardening-fortify-domicile-intruders/>
- <http://www.thelastbastille.com/2016/05/22/dual-layer-encryption-proposal-sidestepping-potential-backdoors/>
- https://en.wikipedia.org/wiki/Kensington_security_slot
- https://en.wikipedia.org/wiki/False_bottom
- <https://youtu.be/luKQKYc-GXE>

Keeping Your Own Counsel

- <http://www.libertyunderattack.com/solutions/>
- <https://en.wikiquote.org/wiki/Truth>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- https://en.wikipedia.org/wiki/Operational_security

- <http://www.survivalblog.com/glossary.html#OPSEC>
- https://en.wikipedia.org/wiki/Information_security
- https://en.wikipedia.org/wiki/Personally_identifiable_information
- <http://www.thelastbastille.com/2015/12/29/socialist-insecurity-how-the-raw-deal-enslaved-americans/>
- http://www.outpost-of-freedom.com/radio/opfarchives/130121_Security_Teams_OPF_Radio.mp3
- <http://www.thelastbastille.com/2012/08/11/the-internet/>
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <http://www.thelastbastille.com/2012/09/15/ostracism/>
- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>
- <http://www.thelastbastille.com/2015/03/02/a-history-of-dragnet-wiretapping/>
- <https://www.urbandictionary.com/define.php?term=snitches%20get%20stitches!>
- <http://www.libertyunderattack.com/court-documents/>
- <http://www.libertyunderattack.com/schuyler-barbeau-2/>
- <http://psychcentral.com/blog/archives/2012/12/07/talking-to-yourself-a-sign-of-sanity/>
- https://en.wikipedia.org/wiki/Social_engineering_%28security%29
- <https://en.wikipedia.org/wiki/Doxing>
- https://en.wikipedia.org/wiki/The_powers_that_be_%28phrase%29
- https://en.wikipedia.org/wiki/Loose_lips_sink_ships

Chilling Dissent: How Government Demonizes Americans

- https://en.wikipedia.org/wiki/Martin_Niem%C3%B6ller
- <http://www.thelastbastille.com/2012/10/17/propaganda/>
- https://en.wikipedia.org/wiki/Chilling_effect
- https://en.wikipedia.org/wiki/Demonizing_the_enemy
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_demonization_of_chris_broughton.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_demonization_of_debra_medina.mp4
- <https://en.wikipedia.org/wiki/Censorship>
- <https://en.wikipedia.org/wiki/Intimidation>

- https://en.wikipedia.org/wiki/Strategic_lawsuit_against_public_participation
- https://en.wikipedia.org/wiki/Malicious_prosecution
- https://en.wikipedia.org/wiki/Freedom_of_speech
- https://en.wikipedia.org/wiki/Freedom_of_the_press
- https://en.wikipedia.org/wiki/Freedom_of_assembly
- https://en.wikipedia.org/wiki/Right_to_petition
- https://en.wikipedia.org/wiki/First_Amendment_to_the_United_States_Constitution
- https://en.wikipedia.org/wiki/Tenth_Amendment_to_the_United_States_Constitution
- <http://www.statutes.legis.state.tx.us/Docs/CN/htm/CN.1.htm>
- https://en.wikipedia.org/wiki/Right_to_keep_and_bear_arms
- https://en.wikipedia.org/wiki/Omnibus_Crime_Control_and_Safe_Streets_Act_of_1968
- https://en.wikipedia.org/wiki/Patriot_Act
- https://en.wikipedia.org/wiki/Aviation_and_Transportation_Security_Act
- https://en.wikipedia.org/wiki/Warrantless_searches_in_the_United_States
- https://en.wikipedia.org/wiki/Section_summary_of_the_Patriot_Act,_Title_II#Section_215:_Access_to_records_and_other_items_under_FISA
- https://en.wikipedia.org/wiki/Transportation_Security_Administration
- https://en.wikipedia.org/wiki/2001_anthrax_attacks
- https://en.wikipedia.org/wiki/Homeland_Security_Act
- https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security#History
- https://en.wikipedia.org/wiki/Cabinet_Secretary#United_States
- https://en.wikipedia.org/wiki/Violent_Radicalization_and_Homegrown_Terrorism_Prevention_Act_of_2007
- https://en.wikipedia.org/wiki/Homegrown_terrorism
- <http://openjurist.org/395/us/444>
- <http://christophercantwell.com/2014/03/15/violently-overthrow-the-government/>
- <http://www.thelastbastille.com/2012/10/03/on-the-duty-of-civil-disobedience/>
- https://en.wikipedia.org/wiki/Imminent_lawless_action
- <https://en.wikipedia.org/wiki/Sedition>

- <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/pdf/USCODE-2012-title18-partI-chap19-sec371.pdf>
- <http://outpost-of-freedom.com/blog/?p=198>
- <http://www.thelastbastille.com/2013/01/15/defamation-legally-defined/>
- <http://www.thelastbastille.com/2013/01/12/libel-legally-defined/>
- <http://www.thelastbastille.com/2013/01/09/slander-legally-defined/>
- <http://libertyunderattack.com/profiling.html>
- https://en.wikipedia.org/wiki/Fusion_center
- https://en.wikipedia.org/wiki/Association_fallacy#Guilt_by_association
- https://en.wikipedia.org/wiki/Police_lineup
- <http://libertyunderattack.com/scenario-training.html>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/jack_bauer_syndrome_-_hollywoods_depiction_of_national_security_law_southern_california_interdisciplinary_law_journal.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/domestic_extremism_lexicon_-_dhss_ia.pdf
- <http://libertyunderattack.com/signs-of-terrorism.html>
- <https://thelastbastille.wordpress.com/2015/04/10/statist-fallacies/>
- <http://www.gpo.gov/fdsys/pkg/PLAW-109publ366/html/PLAW-109publ366.htm>
- https://en.wikisource.org/wiki/National_Defense_Authorization_Act_for_Fiscal_Year_2010/Division_A/Title_XVIII#Title_XVIII
- https://en.wikipedia.org/wiki/Ad_hominem
- https://en.wikipedia.org/wiki/Straw_man
- <http://www.outpost-of-freedom.com/factions.htm>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/terrorism_security_awareness_orientation_for_state_employees_-_commonwealth_of_virginia.pdf
- <http://www.outpost-of-freedom.com/plan.htm>
- <http://www.nbcnews.com/id/37756418>
- <https://docs.google.com/viewerng/viewer?url=https://www.irehr.org/images/stories/pdf/TeaPartyNationalism.pdf>
- <http://www.thelastbastille.com/2014/07/22/state-citizenship-casebook/>
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>

- http://libertyunderattack.com/uploads/3/2/8/2/3282244/addressing_extremism_-_iccr_icar.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/extremism_-_dod_equal_opportunity_management_institute.pdf
- <http://www.gop.com/wp-content/uploads/2012/08/2012GOPPlatform.pdf>
- <http://www.presidency.ucsb.edu/ws/?pid=101962>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_domestic_terrorist_threat_-_background_issues_for_congress_crs.pdf
- <https://youtu.be/ktvHvW-GrvY>
- <https://youtu.be/rg6GvWgWRRc?t=9m36s>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/domestic-extremism-remains-a-persistent-threat-joint_intelligence_bulletin_fbi-dhs.pdf
- <http://www.thelastbastille.com/2012/05/14/who-are-the-terrorists/>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/investigating_terrorism_criminal_extremism_terms_concepts_-_dojs_bja.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/countering_violent_extremism_working_group_homeland_security_advisory_group.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/150415_-_homeland_-_april_19th_is_a_significant_date_to_domestic_extremists_u.s._coast_guard.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/protective_intelligence_bulletin_tmd_03-03-06_fps_-_dhs.pdf
- <https://www.ctc.usma.edu/v2/wp-content/uploads/2013/01/ChallengersFromtheSidelines.pdf>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_power_of_unreason_-_conspiracy_theories_extremism_counter-terrorism_demos.pdf
- <http://outpost-of-freedom.com/blog/?p=1028>
- <https://thelastbastille.wordpress.com/2012/10/21/rules-for-radicals/>
- <http://www.aeinstein.org/english/>
- <https://youtu.be/KQ9w1HHRMQw>
- <http://outpost-of-freedom.com/blog/?p=753>
- <http://www.nps.gov/wwii/index.htm>
- https://en.wikipedia.org/wiki/United_States_federal_government_shut_down_of_2013
- <http://outpost-of-freedom.com/blog/?p=828>

- <http://www.thelastbastille.com/2012/07/09/balkanization/>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/grants_manage ment_unit_grant_application_cfda_97.067_-_fy_2012_nh_department_of_safety.pdf
- https://en.wikipedia.org/wiki/Lenco_BearCat
- https://en.wikipedia.org/wiki/Armoured_personnel_carrier
- <https://www.facebook.com/ThanksButNoTanks>
- <http://tinyurl.com/k2evszzr>
- <http://christophercantwell.com/2013/08/06/concord-police-go-and-get-your-bearcat/>
- <http://www.thelastbastille.com/2013/11/03/the-free-state-project-censorship-debacle/>
- <http://christophercantwell.com/2013/09/03/porcupine-non-grata/>
- <http://www.thelastbastille.com/2014/01/03/ian-bernard-the-man-who-snitched-on-larken-rose/>
- <http://www.thelastbastille.com/2012/12/31/declaration-of-independence/>
- <http://www.gencourt.state.nh.us/rsa/html/LXII/627/627-4.htm>
- <http://www.nh.gov/constitution/billofrights.html>
- https://en.wikipedia.org/wiki/Non_sequitur_%28logic%29
- <http://www.thelastbastille.com/2013/11/05/a-recent-history-of-the-libertarian-position-on-self-defense/>
- <http://www.statutes.legis.state.tx.us/Docs/CN/pdf/CN.1.pdf>
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.9.htm>
- <http://www.outpost-of-freedom.com/gl931221.htm>
- <http://www.thelastbastille.com/2012/07/13/controlled-opposition/>
- <http://www.thelastbastille.com/2011/12/31/problem-reaction-solution-hegelian-dialectic/>
- <http://www.thelastbastille.com/2012/01/04/predictive-programming/>
- https://en.wikipedia.org/wiki/Minority_Report_%28film%29
- <https://en.wikipedia.org/wiki/Psycho-Pass>
- <https://en.wikipedia.org/wiki/Omniscience>
- <https://en.wikipedia.org/wiki/Precognition>
- <https://en.wikipedia.org/wiki/Precrime>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/rightwing_extremism_-_current_economic_and_political_climate_fueling_resurgence_in_radicalization_and_recruitment_-_dhs.pdf

- http://libertyunderattack.com/uploads/3/2/8/2/3282244/leftwing_extremists_likely_to_increase_use_of_cyber_attacks_over_the_coming_decade_-_dhs.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/1.3_are_professional_profilers_better_.mp4
- https://en.wikipedia.org/wiki/Non-governmental_organization
- <http://archive.adl.org/mwd/welcome.html>
- <http://www.adl.org/assets/pdf/combating-hate/Rage-Grows-In-America.pdf>
- <http://www.splcenter.org/get-informed/intelligence-report/browse-all-issues/2010/summer/meet-the-patriots>
- <http://libertyunderattack.com/southern-poverty-law-center.html>
- <http://www.thelastbastille.com/2013/01/08/the-enemies-list/>
- <http://www.thelastbastille.com/2013/09/16/story-of-a-secret-state/>
- <http://www.thelastbastille.com/2013/08/05/are-cops-constitutional/>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/countering_violent_extremism_working_group_homeland_security_advisory_group.pdf
- https://en.wikipedia.org/wiki/Morris_Deas
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/southern_poverty_law_center_-_wellspring_of_manufactured_hate_crc.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/splc_statement_on_dr_ben_carson_splc.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/bounding_the_global_war_on_terrorism_u.s._army_war_college.pdf
- https://en.wikipedia.org/wiki/Enumerated_powers
- https://en.wikipedia.org/wiki/Letter_of_marque
- https://en.wikipedia.org/wiki/Barbary_pirates
- https://en.wikipedia.org/wiki/Security_theater
- <http://www.thelastbastille.com/2014/04/26/administrative-agencies-the-fourth-branch-of-government/>
- <http://www.thelastbastille.com/2014/05/17/larry-myers-an-ignored-political-prisoner/>
- <http://outpost-of-freedom.com/blog/?p=892>
- <http://outpost-of-freedom.com/blog/?p=1114>
- <http://www.npr.org/2011/07/12/137708256/what-the-new-normal-means-for-americans>
- <http://www.outpost-of-freedom.com/okc0501.htm>
- <http://libertyunderattack.com/signs-of-terrorism.html>

- http://libertyunderattack.com/uploads/3/2/8/2/3282244/intent_to_deceive_nature.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/tsa_should_limit_future_funding_for_behavior_detection_activities_gao.pdf
- <http://www.gpoaccess.gov/911/pdf/fullreport.pdf>
- <http://www.txdps.state.tx.us/IntelligenceCounterterrorism/fusion.htm>
- <http://rocic.com/>
- <http://www.riss.net/>
- <http://texasimpact.org/PDFs/TexasImpactFusionCenterReport.pdf>
- https://en.wikipedia.org/wiki/Visible_Intermodal_Prevention_and_Response_team
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/viper_teams_greyhound_bus_stations_-_abc_tampa.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/viper_teams_conduct_truck_inspections_on_i-20_-_atlanta_ga_wsb-tv.mp4
- https://www.aclu.org/sites/default/files/field_document/jus14-warcomeshome-report-web-rel1.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/no_real_threat_-_the_pentagons_secret_database_on_peaceful_protest_aclu.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/dods_level_1_anti-terrorism_awareness_training_aclu.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/force_protection_advisory_09-01_u.s._army_reserve.pdf
- https://en.wikipedia.org/wiki/Pier_57
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/surveillance_drone_footage_vanguard_defense_industries.mp4
- <https://en.wikipedia.org/wiki/Blacklisting>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/mikey_hicks_on_the_early_show_cbs.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/rahm_emanuel_speaks_at_the_brady_centers_stand_up_for_a_safe_america_-_no_fly_list_no_gun_buy_brady_campaign.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/riyanna_18_months_receives_apology_from_jetblue_for_accidently_being_put_on_the_no_fly_list_wbpf.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/how_it_works_-_tsa.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/z_backscatter_vans_-_zbvs_american_science_engineering.mp4

- http://libertyunderattack.com/uploads/3/2/8/2/3282244/mini_z_american_science_engineering.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/future_attribute_screening_technology_-_dhs.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/criminal_street_gang_identification_interdiction_north_texas_hidta_joint_training_initiative.pdf
- <http://www.statutes.legis.state.tx.us/Docs/CR/htm/CR.61.htm>
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.71.htm>
- <http://www.gpo.gov/fdsys/pkg/CFR-2014-title28-vol1/pdf/CFR-2014-title28-vol1-part23.pdf>
- <http://www.txdps.state.tx.us/txgangs/txgangoverview.pdf>
- https://en.wikipedia.org/wiki/Involuntary_commitment
- <http://www.statutes.legis.state.tx.us/Docs/CN/htm/CN.1.htm>
- <http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.573.htm>
- <http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.574.htm>
- <http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.571.htm>
- https://www.rutherford.org/publications_resources/on_the_front_lines/victory_circuit_court_orders_brandon_raub_released_dismisses_case_against_m
- <https://en.wikipedia.org/wiki/Psikhushka>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/online_person_a_management_service_federal_business_opportunities.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_art_of_deception_-_training_for_a_new_generation_of_online_cover_operations_gchq.pdf
- https://en.wikipedia.org/wiki/Digital_footprint
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/deriving_concept-based_user_profiles_from_search_engine_logs_hong_kong_university.pdf
- http://www.slate.com/articles/news_and_politics/victory_lab/2012/01/the_co_op_and_the_data_trust_the_dnc_and_rnc_get_into_the_data_mining_business.html
- <https://en.wikipedia.org/wiki/Metadata>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/an_introduction_to_recorded_future.mp4
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/recorded_future_-_a_white_paper_on_temporal_analytics.pdf

- https://en.wikipedia.org/wiki/Anne_Tompkins
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/ann_tompkins_doj_press_release_33a183a11.pdf
- <http://www.thelastbastille.com/2012/05/14/who-are-the-terrorists/>
- https://en.wikipedia.org/wiki/Freedom_of_speech
- https://en.wikipedia.org/wiki/Freedom_of_the_press
- https://en.wikipedia.org/wiki/Freedom_of_assembly
- https://en.wikipedia.org/wiki/Right_to_petition
- <http://c4ss.org/intro-to-security-culture>
- <https://en.wikipedia.org/wiki/Kulak>
- https://en.wikipedia.org/wiki/Russian_Soviet_Federative_Socialist_Republic
- <https://en.wikipedia.org/wiki/Parisian>
- https://en.wikipedia.org/wiki/German_military_administration_in_occupied_France_during_World_War_II
- <https://youtu.be/cvToBjNamUQ>
- <http://libertyunderattack.com/solutions.html>
- https://en.wikipedia.org/wiki/Bruce_Schneier
- https://youtu.be/CGd_M_CpeDI?t=9m12s
- <https://ssd.eff.org/en/glossary/risk-analysis>
- <https://ssd.eff.org/en/glossary/threat>
- <https://ssd.eff.org/en/glossary/adversary>
- https://en.wikipedia.org/wiki/Aton_Edwards
- <http://wp.me/p1yWDL-Go>
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/the_modern_militia_movement_-_miac_strategic_report.pdf
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/1_bja_zip_file.zip
- <http://libertyunderattack.com/signs-of-terrorism.html>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://www.thelastbastille.com/2013/09/16/story-of-a-secret-state/>
- <https://ssd.eff.org/>
- <https://en.wikipedia.org/wiki/Off-the-grid>
- <http://libertyunderattack.com/solutions.html>
- <http://voluntarysociety.org/action/goinggalt.html>
- https://en.wikipedia.org/wiki/Perpetual_traveler

- http://libertyunderattack.com/uploads/3/2/8/2/3282244/three_articles_on_the_vonu_strategy_liberty_magazine_1987.pdf
- <http://www.thelastbastille.com/2013/09/02/the-activist-legal-defense-fund-scam/>
- <http://www.thelastbastille.com/2012/02/23/leaderless-resistance-an-overview/>
- <http://destructables.org/node/54>
- <http://www.thelastbastille.com/2014/03/19/they-dont-make-em-like-they-used-to/>
- <http://www.thelastbastille.com/2013/08/09/the-production-of-security/>
- <http://outpost-of-freedom.com/blog/?p=1102>
- <http://outpost-of-freedom.com/blog/?p=1109>
- <http://www.thelastbastille.com/2014/07/19/ecodefense/>
- http://www.outpost-of-freedom.com/radio/bel/130328_Privacy_Part_2.mp3
- <http://www.thelastbastille.com/2015/01/01/reclaiming-unclaimed-property-from-the-government/>
- https://en.wikipedia.org/wiki/Pen_name
- https://en.wikipedia.org/wiki/Malcolm_X#Prison
- <http://libertyunderattack.com/>
- <http://www.libertyunderattack.com/profiling/>

Fanciful Notices: Should You Post a Warning Sign on Your Property?

- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>
- <https://youtu.be/wl3PG4LdYoU>
- <http://www.thelastbastille.com/2013/03/16/the-politics-of-heroin/>
- <http://www.thelastbastille.com/2015/07/30/a-primer-on-homeschooling-how-to-resist-centrally-planned-indoctrination/>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- <http://www.thelastbastille.com/2015/06/27/we-dont-live-in-a-police-state/>
- <http://www.signs.com/design>
- <https://www.signs.com/aluminum/>
- <http://www.thelastbastille.com/2016/01/13/blending-art-grey-man/>
- <http://www.thelastbastille.com/2013/05/13/how-to-make-your-car-inconspicuous/>

- <http://www.thelastbastille.com/2013/11/29/filming-government-agents-does-not-work/>
- <http://www.thelastbastille.com/2015/05/11/chilling-dissent-how-government-demonizes-americans/>
- https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution#Text
- https://en.wikipedia.org/wiki/Ninth_Amendment_to_the_United_States_Constitution#Text
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>
- <http://www.statutes.legis.state.tx.us/Docs/CN/htm/CN.1.htm>
- <http://www.thelastbastille.com/2015/11/08/limited-carjacking-a-simile/>
- <http://www.thelastbastille.com/2015/03/02/a-history-of-drag-net-wiretapping/>
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- https://en.wikipedia.org/wiki/Jurisdictional_arbitrage
- https://en.wikipedia.org/wiki/Color_%28law%29
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title18/html/USCODE-2012-title18-partI-chap13-sec242.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title42/html/USCODE-2012-title42-chap21-subchapI-A-sec1997a.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title42/html/USCODE-2012-title42-chap136-subchapIX-partB-sec14141.htm>
- <https://www.gpo.gov/fdsys/pkg/USCODE-2012-title42/html/USCODE-2012-title42-chap21-subchapI-A-sec1997.htm>
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.39.htm>
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.12.htm>
- <http://www.thelastbastille.com/tax-ban-or-regulate/>
- <https://www.justice.gov/crt/deprivation-rights-under-color-law>
- https://www.fbi.gov/about-us/investigate/civilrights/color_of_law
- <http://www.libertyunderattack.com/suing-the-government-does-not-work-lawsuits-are-not-useful-for-securing-your-liberty/&>
- <http://www.wilco.org/default.aspx?tabid=222>
- <https://www.justice.gov/usao/resources/crime-victims-rights-ombudsman/filing-complaint>

- <http://www.libertyunderattack.com/bibliography-for-why-suing-the-government-doesnt-work/>
- <http://www.statutes.legis.state.tx.us/Docs/CP/htm/CP.9.htm>
- <http://www.statutes.legis.state.tx.us/Docs/CP/htm/CP.11.htm>
- <http://idioms.thefreedictionary.com/hedge+bets>
- <https://tinyurl.com/o48fbnl>
- <http://www.courts.state.tx.us/rules/TRE/tre-all-010107.pdf>
- https://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution#Exceptions_to_the_warrant_requirement
- https://en.wikipedia.org/wiki/Legal_opportunism
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <http://www.thelastbastille.com/2012/06/25/refusing-consent-the-power-of-non-compliance/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- https://en.wikipedia.org/wiki/Wishful_thinking
- <http://www.thelastbastille.com/2016/03/02/sifting-wheat-chaff-value-skepticism/>
- <http://www.thelastbastille.com/2015/05/10/the-law-is-a-racket/>

How to Roleplay Police Interrogations

- http://youtu.be/bNUQOHKhf_M
- <http://youtu.be/KQ9w1HHRMQw>
- <http://youtu.be/rg6GvWgWRRc>
- <http://www.thelastbastille.com/2012/11/02/serious-self-defense/>
- <http://www.thelastbastille.com/2013/08/05/are-cops-constitutional/>
- <http://www.thelastbastille.com/2012/10/17/propaganda/>
- http://www.outpost-of-freedom.com/radio/bel/130207_Conditioning.mp3
- https://en.wikipedia.org/wiki/Exculpatory_evidence
- https://en.wikipedia.org/wiki/Miranda_warning
- <http://youtu.be/i8z7NC5sgik>
- <https://tinyurl.com/o48fbnl>
- <http://www.courts.state.tx.us/rules/TRE/tre-all-010107.pdf>
- https://en.wikipedia.org/wiki/Ignorantia_juris_non_excusat
- <http://www.thelastbastille.com/2014/05/24/woe-unto-you-lawyers/>

- <http://www.thelastbastille.com/2013/09/16/story-of-a-secret-state/>
- <https://www.youtube.com/playlist?list=PLQKn6VyrLIpfafKwYkEecRXDZ-6l-ZxRF>
- <http://youtu.be/yqMjMPIXzdA>
- <http://www.urbandictionary.com/define.php?term=lawyer%20up>
- <https://en.wikipedia.org/wiki/Safeword>
- https://en.wikipedia.org/wiki/Prisoner%E2%80%99s_dilemma
- <http://www.thelastbastille.com/2014/07/25/a-primer-on-state-citizenship/>
- <http://youtu.be/Jg1YcVvLmqU>
- <http://www.newgrounds.com/collection/thenegotiator>
- <http://www.zap.ca/>
- <http://www.thelastbastille.com/2013/11/29/filming-government-agents-does-not-work/>
- <http://www.assertrights.com/>
- <http://www.thelastbastille.com/2013/08/05/are-cops-constitutional/>
- <http://www.thelastbastille.com/2012/10/16/victim-mentality/>
- <http://www.survivalthinktank.com/2011/11/grey-man-directive.html>
- https://en.wikipedia.org/wiki/Making_false_statements
- <http://youtu.be/08fZQWjDVKE?t=18m10s>

Blending In: The Art of the Grey Man

- <http://www.thelastbastille.com/2012/10/31/disguise-techniques/>
- <http://www.thelastbastille.com/2015/05/11/chilling-dissent-how-government-demonizes-americans/>
- <http://www.libertyunderattack.com/the-freedom-umbrella-of-direct-action-second-edition/>
- <http://fprnradio.com/liberty-under-attack-091315/>
- <http://www.thelastbastille.com/2015/09/01/modeling-threats-and-analyzing-risk-a-rebuttal-against-doom-porn/>
- <https://www.urbandictionary.com/define.php?term=grey+man>
- <http://westernrifleshooters.blogspot.com/2007/05/next-steps-grey-man.html>
- <https://3.bp.blogspot.com/-M25zPQtim6A/UjO4jA7jQRI/AAAAAAAAAOW/oxDryaquVVY/s1600/Duck+Picture.jpg>

- <http://www.theprepperjournal.com/2014/07/26/grey-man-concept-neighbor/>
- <http://www.thelastbastille.com/2012/08/07/openly-carrying-firearms/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://www.artofmanliness.com/2015/02/05/how-to-develop-the-situational-awareness-of-jason-bourne/>
- https://en.wikipedia.org/wiki/Everyday_carry
- <http://www.thelastbastille.com/2012/10/06/individuality/>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- https://youtu.be/4cm_4PHduUs
- https://en.wikipedia.org/wiki/3_Percenters
- http://ecx.images-amazon.com/images/I/41xIcOeT3jL._SY300_.jpg
- <http://www.thelastbastille.com/2013/05/13/how-to-make-your-car-inconspicuous/>
- <http://www.thelastbastille.com/2012/11/04/methods-of-disguise/>
- <https://www.washingtonpost.com/archive/politics/1995/03/29/hospitality-sweet/91c11246-272a-4005-bda3-8e8eee07a76e/>
- https://farm8.staticflickr.com/7216/6905827198_0b10b0a168.jpg
- <http://openjurist.org/516/us/442>
- <http://www.thelastbastille.com/2014/09/19/stealing-your-life-away-the-threat-of-civil-asset-forfeiture/>
- <http://jimbovard.com/blog/2015/10/09/wash-posts-wittiest-column-ends-captured-my-supreme-court-eviction/>
- <https://tinyurl.com/politicalfieldtrips>
- <http://www.thelastbastille.com/2012/10/31/disguise-techniques/>
- <http://www.thelastbastille.com/2012/12/19/1984/>
- <http://graywolfsurvival.com/79/how-to-gray-man-shft/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- https://en.wikipedia.org/wiki/Small_talk
- <http://www.thefreedictionary.com/noncommittal>
- <https://en.wikipedia.org/wiki/Sprezzatura>
- <http://www.theprepperjournal.com/2013/04/15/situational-awareness-for-the-focus-challenged-prepper/>
- <https://en.wikipedia.org/wiki/Mindfulness>
- <http://www.artofmanliness.com/2014/01/30/your-concentration-training-program-11-exercises-that-will-strengthen-your-attention/>
- <http://graywolfsurvival.com/2173/using-kims-game-to-train-your-mind-for-survival/>

- <http://www.survivalpunk.com/how-to-be-a-gray-man/>
- <http://www.thelastbastille.com/2013/05/12/keeping-up-with-the-joneses/>
- <http://www.survivalthinktank.com/2011/11/grey-man-directive.html>
- <http://www.edcitems.com/about>
- <https://web.archive.org/web/20150423163102/http://www.everycitize.nasoldier.org/id12.html>
- https://en.wikipedia.org/wiki/Bug-out_bag
- http://survivalblog.com/letter_re_survivalist_media-a/
- <http://graywolfsurvival.com/2551/what-should-you-have-in-your-everyday-carry-edc-gear/>
- <https://www.youtube.com/user/nutnfancy/videos?view=0>
- <https://youtu.be/jRfWyaNRKsE>
- <http://www.libertyunderattack.com/a-day-in-the-life-of-the-average-joe-citizen/>
- https://en.wikipedia.org/wiki/Parachute_cord
- <https://en.wikipedia.org/wiki/Multi-tool>
- <https://www.instagram.com/p/c7UWe3MdNL/>
- <http://www.libertyunderattack.com/solutions/>
- http://www.huffingtonpost.com/2014/10/30/ghosting-dating-_n_6028958.html
- <https://en.wikipedia.org/wiki/Breakup>
- <http://www.thelastbastille.com/2013/09/26/reborn-in-canada/>
- <http://www.thelastbastille.com/2015/03/02/a-history-of-dragnet-wiretapping/>
- <http://www.thelastbastille.com/2012/07/12/alternative-media/>
- <http://www.thelastbastille.com/2013/03/06/mind-your-own-business/>

How to Make Your Car Inconspicuous

- <http://www.thelastbastille.com/2015/03/02/a-history-of-dragnet-wiretapping/>
- <http://www.thelastbastille.com/2013/05/12/keeping-up-with-the-joneses/>
- https://en.wikipedia.org/wiki/Sport_utility_vehicle
- <https://www.youtube.com/user/NsaneSk8er007/videos?view=0>
- <http://survival4christians.blogspot.com/2010/08/become-gray-man.html>

- <http://www.thelastbastille.com/2012/11/02/serious-self-defense/>
- <http://www.thelastbastille.com/category/the-establishment/>
- <https://en.wikipedia.org/wiki/Off-roading>
- https://en.wikipedia.org/wiki/Mud_bogging
- https://en.wikipedia.org/wiki/Plain_view_doctrine
- http://libertyunderattack.com/uploads/3/2/8/2/3282244/terrorist_screening_center_police_training_video_police_state_4.mp4
- <https://youtu.be/yqMjMPIXzdA>
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <http://www.thelastbastille.com/2012/05/10/evil-in-itself-or-just-forbidden/>
- <http://www.thelastbastille.com/2012/10/03/on-the-duty-of-civil-disobedience/>
- <https://tinyurl.com/civilassetforfeiture>

Home Hardening: How to Fortify Your Domicile Against Intruders

- https://en.wikipedia.org/wiki/Cider_Bill_of_1763
- https://en.wikipedia.org/wiki/Castle_doctrine
- <http://www.commonlii.org/int/cases/EngR/1572/333.pdf>
- https://en.wikipedia.org/wiki/Stand-your-ground_law
- https://en.wikipedia.org/wiki/Duty_to_retreat
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.9.htm>
- https://en.wikipedia.org/wiki/Joe_Horn_shooting_controversy
- <http://www.statutes.legis.state.tx.us/Docs/PE/htm/PE.9.htm>
- <http://tiny.cc/dragnetwiretapping>
- <http://tiny.cc/civilforfeiture>
- <http://www.libertyunderattack.com/court-documents/>
- <https://youtu.be/t4JeaYwdjTY>
- https://en.wikipedia.org/wiki/Safety_and_security_window_film
- <https://www.amazon.com/s?ie=UTF8&page=1&rh=i%3Aaps%2Ck%3Awindow%20safety%20film>
- https://en.wikipedia.org/wiki/Safety_glass
- https://en.wikipedia.org/wiki/Bulletproof_glass
- http://www.ebay.com/sch/i.html?_nkw=bulletproof%20glass&clk_rvr_id=1042301739423&mfe=search
- <https://youtu.be/96x2tO9Xuxw>

- https://youtu.be/_ZDAW4K8EWg
- https://en.wikipedia.org/wiki/Solid_wood#Solid_wood_vs._hollow_wood
- <http://www.katybar.com/Katy-Bar-Features.cfm>
- <https://youtu.be/VShhg9uCjoo>
- <http://www.katybar.com/shop/select-type-new-2.cfm>
- <https://www.globalsecurityexperts.com/products/security-door-brace.html>
- <https://youtu.be/leZSx6uWofc>
- <https://www.timbercompositedoors.com/>
- <https://youtu.be/J233yEmYauw>
- <https://youtu.be/AfxVpsubIHE>
- http://www.ehow.com/how_12074899_diy-cinder-block-retaining-walls-rebar-concrete.html
- <http://www.koiphen.com/forums/showthread.php?72831-Average-price-for-Concrete-Block>
- <http://www.homedepot.com/p/Weyerhaeuser-1-2-in-x-10-ft-Rebar-05366/202094293>
- <http://www.homedepot.com/p/Quikrete-80-lb-Concrete-Mix-110180/100318511>
- https://en.wikipedia.org/wiki/Heist_film
- <https://youtu.be/wl3PG4LdYoU>
- <https://mises.org/library/short-history-man-progress-and-decline>
- https://youtu.be/KOS6grr_6iY
- <http://www.thelastbastille.com/2013/03/12/pranks-2/>
- https://en.wikipedia.org/wiki/Safe_room
- <http://www.risingsbunkers.com/safe-room-sizes-pricing/>
- <https://tinyurl.com/selfdefense4me>
- <https://youtu.be/WKJhwy1l640>
- <https://en.wikipedia.org/wiki/Demand>
- <http://www.thelastbastille.com/2016/06/14/vonu-search-personal-freedom/>

Interpersonal Diplomacy: The Value of Keeping the Peace

- <https://en.wikipedia.org/wiki/Diplomacy>
- <https://en.wikipedia.org/wiki/Etiquette>
- <http://www.thelastbastille.com/2013/11/15/standing-under-freedom/>

- <http://www.merriam-webster.com/dictionary/diplomacy>
- <http://www.thelastbastille.com/2012/10/06/live-and-let-live-the-beauty-of-individuality/>
- <http://www.thelastbastille.com/2014/08/10/how-to-roleplay-a-police-interrogation/>
- <http://www.libertyunderattack.com/luca-radio-2-14-16-direct-action-series-6-non-violent-communication-relationship-anarchy/>
- <http://www.thelastbastille.com/2016/01/13/blending-art-grey-man/>
- <https://tinyurl.com/politicalfieldtrips>
- <http://www.thelastbastille.com/2012/08/06/debating-does-not-work/>
- <http://www.libertyunderattack.com/libertarian-role-modeling-how-to-outgrow-the-state-part-2/>
- <http://fprnradio.com/disassociation-nation-121815/>
- <https://tinyurl.com/nullifythejury>
- <http://www.thelastbastille.com/2012/07/09/balkanization/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://www.thelastbastille.com/2013/02/13/may-you-live-in-interesting-times/>
- <http://outpost-of-freedom.com/blog/?p=823>
- <http://outpost-of-freedom.com/blog/?p=1349>
- <http://freekeene.com/2009/07/21/neighbors-helping-neighbors/>
- <http://www.thelastbastille.com/2014/03/01/thomas-jefferson-had-neither-his-pocket-picked-nor-his-legs-broken/>

Disingenuous Activists! Why Leaderless Resistance is Preferable to Formal Organizations

- <http://www.thelastbastille.com/2013/09/22/how-to-disappear-in-america/>
- <http://tiny.cc/vetting>
- <https://tinyurl.com/emailkeywords>
- <http://tiny.cc/warningsign>
- <https://en.wikipedia.org/wiki/Populism>
- <http://www.thelastbastille.com/2016/01/26/democracy-in-america/>
- <http://www.carolmoore.net/articles/secession-strategy.html>
- <http://www.thelastbastille.com/2015/07/13/coup-detat-a-practical-handbook/>

- https://en.wikipedia.org/wiki/Social_movement
- https://en.wikipedia.org/wiki/Political_movement
- <https://tiny.cc/individuality>
- <http://www.thelastbastille.com/2015/07/16/reformism-does-not-work-a-critique-of-political-activism/>
- https://youtu.be/jiAThxUM_Mg
- <http://tiny.cc/homeschoolingprimer>
- <http://tiny.cc/skepticism>
- <https://tinyurl.com/politicalfieldtrips>
- <http://www.collinsdictionary.com/dictionary/english/politicking>
- <http://www.thelastbastille.com/2012/12/07/anatomy-of-the-state/>
- https://en.wikipedia.org/wiki/Force_multiplication
- <http://cspoa.org/about/>
- <http://www.thelastbastille.com/2016/02/26/texas-constitutional-sheriff-letters-2013/>
- <http://tenthamendmentcenter.com/about/>
- <http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=84R&Bill=HB910>
- <http://tiny.cc/doomporn>
- <http://tiny.cc/skepticism>
- <http://www.iiipercentidaho.org/about/>
- <http://tiny.cc/skepticism>
- <http://tiny.cc/legaldefensefundscam>
- <http://www.thelastbastille.com/2015/11/28/bitcoiners-betrayed-lobbyists-sell-out-to-the-government/>
- <https://youtu.be/X2PHF5GPXLg?t=1h18m30s>
- <https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7>
- <http://www.thelastbastille.com/2013/11/03/the-free-state-project-censorship-debacle/>
- <http://www.nh.gov/constitution/billofrights.html>
- <http://www.thelastbastille.com/2014/01/03/ian-bernard-the-man-who-snitched-on-larken-rose/>
- https://en.wikipedia.org/wiki/Purges_of_the_Communist_Party_of_the_Soviet_Union
- <http://www.thelastbastille.com/2012/12/19/1984/>
- <http://christophercantwell.com/2015/09/19/goodbye-cuck-talk-live/>
- <https://freestateproject.org/blogs/free-state-project-officially-announces-20000-signers-100-reached>

- <https://freestateproject.org/blogs/free-state-project-statement-regarding-ian-freeman-and-free-talk-live>
- <http://freekeene.com/2016/03/22/free-talk-lives-press-release-about-fbi-raid/>
- <http://nhlibertyforum.com/>
- <http://porcfest.com/>
- <http://www.thelastbastille.com/2014/01/03/ian-bernard-the-man-who-snitched-on-larken-rose/>
- <http://www.thelastbastille.com/2016/03/20/the-bundy-affair-2014/>
- <http://www.operationmutualdefense.org/>
- <https://www.oathkeepers.org/oath-keepers-national-call-to-action-help-us-protect-the-protectors-by-guarding-recruiting-and-reserve-centers/>
- <https://tinyurl.com/endingwar>
- <https://youtu.be/D6kPEdjQJM8>
- <http://www.thelastbastille.com/2016/04/11/absorption-dilution-jpfo-saf/>
- <http://jpfo.org/filegen-a-m/about.htm>
- <https://www.saf.org/mission/>
- https://en.wikipedia.org/wiki/Personally_identifiable_information
- <http://www.thelastbastille.com/2016/02/24/mark-kessler-an-enemy-of-liberty/>
- http://www.outpost-of-freedom.com/documents/III_BOG_Application.pdf
- https://en.wikipedia.org/wiki/The_Alan_Colmes_Show
- https://en.wikipedia.org/wiki/Honeypots_in_espionage_fiction
- <http://tiny.cc/chillingdissent>
- <http://www.libertyunderattack.com/texans-for-accountable-government-tag-meeting-92815/>
- <https://youtu.be/qPFxybzPQT0>
- <https://youtu.be/e014SiPLj4I?t=3m2s>
- <https://youtu.be/vbpeKg4YDjY>
- <http://www.tagtexas.org/about>
- <http://www.standwithlaura.com/>
- <https://tinyurl.com/slvjustus>
- <http://www.thelastbastille.com/2016/03/26/operation-patriot-rally-point-2015/>
- <https://youtu.be/D1Xg71zzY5o?t=6m09s>
- <http://tiny.cc/keepthepeace>
- <https://tinyurl.com/wclp2015>

- https://en.wikipedia.org/wiki/Agorism#Opposition_to_22Partyarchy.22
- <https://www.lewrockwell.com/podcast/85-david-nolan-what-happened-to-the-libertarian-party/>
- <http://www.libertyunderattack.com/behind-enemy-lines-the-dangers-of-the-libertarian-party/>
- <https://tinyurl.com/onlyonpaper>
- <https://tinyurl.com/fakejudges>
- <http://www.libertyunderattack.com/the-statist-turf-war-concluded/>
- <https://www.hslda.org/about/>
- <http://www.thsc.org/about-thsc/>
- <http://www.ij.org/about-us/>
- <https://fee.org/about/>
- <https://mises.org/about-mises>
- <http://isil.org/about/>
- <http://www.nhliberty.org/about>
- https://en.wikipedia.org/wiki/New_Hampshire_General_Court
- <https://tiny.cc/grassrootslobbying>
- <https://radiofreeredoubt.com/about/>
- <http://alexansary.tv/>
- <https://tinyurl.com/keepyourcounsel>
- <https://tinyurl.com/emailkeywords>
- <https://network23.org/infiltrators/2014/08/27/snitch-jacketing-in-our-movements/>
- <https://en.wikipedia.org/wiki/Doxing>
- <http://tiny.cc/legaldefensefundscam>
- <http://tiny.cc/chillingdissent>
- <http://www.thelastbastille.com/2012/02/23/leaderless-resistance-an-overview/>
- <http://destructables.org/node/54>
- https://en.wikipedia.org/wiki/Mutual_aid_%28organization_theory%29
- https://en.wikipedia.org/wiki/Plausible_deniability
- http://www.outpost-of-freedom.com/radio/opfarchives/130121_Security_Teams_OPF_Radio.mp3
- <https://youtu.be/MwTBq9y3nFI>
- <https://tiny.cc/individuality>
- <http://www.thelastbastille.com/2014/07/19/ecodefense/>

- <http://christophercantwell.com/2015/01/24/7-steps-becoming-celebritarian/>
- <http://www.thelastbastille.com/2013/07/15/signs-you-may-be-addicted-to-a-patriot-rockstar/>
- <http://www.thelastbastille.com/2013/09/16/story-of-a-secret-state/>
- <http://www.thelastbastille.com/2012/10/17/propaganda/>
- <http://www.thelastbastille.com/2016/02/10/committees-of-safety-an-american-tradition/>
- <http://www.liberaterva.com/about/>
- <http://thehoustonfreethinkers.com/>

Your Are Known By the Company You Keep: How to Choose Your Allies Wisely

- <https://survivalblog.com/precepts/>
- https://en.wikipedia.org/wiki/Freedom_of_association#Libertarian
- <http://www.thelastbastille.com/2016/02/23/a-reply-to-the-current-critiques-formulated-against-hoppes-argumentation-ethics/>
- <http://www.thelastbastille.com/2012/10/06/live-and-let-live-the-beauty-of-individuality/>
- https://en.wikipedia.org/wiki/Freedom_of_contract
- <http://www.thelastbastille.com/2012/11/26/interpersonal-diplomacy-the-value-of-keeping-the-peace/>
- https://en.wikipedia.org/wiki/Freedom_of_assembly
- <http://www.thelastbastille.com/2016/02/02/a-covenant-with-death-and-an-agreement-with-hell-a-review-of-the-united-states-constitution/>
- <http://www.heritage.org/constitution/amendments/1/essays/141/freedom-of-assembly-and-petition>
- <http://www.statutes.legis.state.tx.us/Docs/SDocs/THETEXASCONSTITUTION.pdf>
- <http://www.thelastbastille.com/2015/05/11/chilling-dissent-how-government-demonizes-americans/>
- <http://www.libertyunderattack.com/solutions/>
- <http://www.libertyunderattack.com/the-libertarian-case-for-judicial-transparency/>
- <http://www.libertyunderattack.com/william-wolf/>
- <http://outpost-of-freedom.com/blog/?p=1105>

- <http://outpost-of-freedom.com/Vortex.htm>
- <http://www.thelastbastille.com/2012/07/13/controlled-opposition/>
- <http://www.libertyunderattack.com/schuyler-barbeau-2/>
- <http://outpost-of-freedom.com/blog/?p=1296>
- <http://www.thelastbastille.com/tax-ban-or-regulate/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://outpost-of-freedom.com/Vortex.htm>
- http://www.outpost-of-freedom.com/radio/bel/150124_BEL_Internet_Friends_and_Rumor_Mill.mp3
- <https://youtu.be/89XMFY0I4w>
- <http://www.thelastbastille.com/2012/09/13/vetting/>
- <http://www.thelastbastille.com/2012/09/15/ostracism/>
- https://en.wikipedia.org/wiki/Marginal_utility
- <http://www.thelastbastille.com/2012/10/06/live-and-let-live-the-beauty-of-individuality/>
- <http://www.thelastbastille.com/2014/07/09/i-pencil/>
- <http://www.meetup.com/>
- <https://tinyurl.com/politicalfieldtrips>
- <http://www.thelastbastille.com/2013/05/13/how-to-make-your-car-inconspicuous/>
- <http://www.thelastbastille.com/2016/01/13/blending-art-grey-man/>
- <http://www.thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://www.libertyunderattack.com/austin-municipal-court-docket-session-10-05-2015/>
- <http://www.libertyunderattack.com/texans-for-accountable-government-tag-meeting-92815/>
- <http://www.libertyunderattack.com/williamson-county-libertarian-party-chapter-meeting-10-12-15/>
- <http://www.thelastbastille.com/2012/11/26/interpersonal-diplomacy-the-value-of-keeping-the-peace/>
- <http://www.thelastbastille.com/2012/11/02/serious-self-defense/>
- <http://www.thelastbastille.com/2015/03/19/education-free-compulsory/>
- <http://www.thelastbastille.com/2012/11/06/50-secrets-for-picking-up-girls/>
- <http://www.thelastbastille.com/2012/08/06/debating-does-not-work/>
- http://psychology.wikia.com/wiki/Family_of_origin

- <https://youtu.be/0z-fhCFkISM?t=19m14s>
- <https://youtu.be/I-YMMd1xKIM?t=22m59s>
- <http://www.libertyunderattack.com/libertarian-role-modeling-how-to-outgrow-the-state/>
- <http://www.libertyunderattack.com/libertarian-role-modeling-how-to-outgrow-the-state-part-2/>
- <http://www.thelastbastille.com/2013/09/02/the-activist-legal-defense-fund-scam/>
- <http://www.thelastbastille.com/2014/03/22/some-thoughts-on-george-hemmingsers-confessions/>
- <http://www.thelastbastille.com/category/ron-paul-lovefest/>
- <http://www.thelastbastille.com/2013/08/23/a-revelation-of-the-method/>
- <http://outpost-of-freedom.com/blog/?p=828>
- <http://outpost-of-freedom.com/blog/?p=1039>
- <http://www.thelastbastille.com/2016/02/24/mark-kessler-an-enemy-of-liberty/>
- <http://www.thelastbastille.com/2013/09/22/how-to-disappear-in-america/>
- <http://www.thelastbastille.com/2012/07/05/compartamentalization/>
- <https://youtu.be/dPRQLkQf2A?t=12m50s>
- <http://www.aesopfables.com/cgi/aesop1.cgi?sel&TheAssandhisPurchaser2>

May You Live in Interesting Times...

- <http://www.thelastbastille.com/2012/07/13/controlled-opposition/>
- <http://www.thelastbastille.com/2012/01/11/internal-balkanization-infighting/>
- <http://www.thelastbastille.com/2012/10/06/individuality/>
- <http://www.thelastbastille.com/2012/06/24/yhtom-reading-list/>
- <http://www.thelastbastille.com/2012/03/30/the-last-bastille-podcast-47-you-have-tread-on-me/>
- <http://www.thelastbastille.com/2012/09/18/committee-of-safety-common-law-court-cos-clc/>
- <http://www.thelastbastille.com/2012/07/25/no-more-messiahs/>
- <http://www.thelastbastille.com/2012/09/19/mascarenas-v-stachowiak-cos-clc-verdict-110401/>

- <http://freedomfighterradio.net/>
- <http://www.thelastbastille.com/2012/11/26/interpersonal-diplomacy/>
- <http://thelastbastille.com/2012/11/23/keeping-your-own-counsel/>
- <http://wramsite.com/>
- <http://www.thelastbastille.com/2012/10/08/swan-v-light-cos-clc-unanswered-indictment-120201/>
- <http://www.thelastbastille.com/2012/12/10/baez-v-rudkowski-cos-clc-unanswered-indictment-120301/>
- <http://wearechange.org/>
- <http://www.thelastbastille.com/2013/01/31/robert-handel-aka-green-mountain-patriot-wall-of-shame-cos-clc/>
- <http://www.thelastbastille.com/2013/02/02/james-sims-aka-j-sims-wall-of-shame-cos-clc/>
- <http://www.thelastbastille.com/2012/08/09/the-moon-is-a-harsh-mistress/>
- <http://www.thelastbastille.com/2013/02/08/mark-koenig-aka-smiter13-wall-of-shame-cos-clc/>
- <http://rantinglouiebee.blogspot.com/>
- <http://www.thelastbastille.com/2013/02/10/washington-state-militia-statement-regarding-mark-koenig/>
- https://youtu.be/_r2wYNBxus8
- <http://www.thelastbastille.com/2012/09/15/ostracism/>
- <http://www.best-childrens-books.com/company-you-keep.html>
- <http://www.thelastbastille.com/2012/07/12/alternative-media/>
- <http://thelastbastille.com/2012/08/13/carnival-of-distractions/>
- https://en.wikipedia.org/wiki/May_you_live_in_interesting_times