Privacy for Identities: The Art of Pseudonymity

A thought guide to maintaining operational security for your digital identities.

Written for cypherpunks, privacy advocates, hackers, and anyone else with an interest in identities, surveillance, personal privacy, and operational security.

Independently Authored
Cypher
@CryptoCypher

Pre-release version published 2019-04-04

Syllabus: The Outline

Part One: The Introduction

Introduction

Part Two: Considering Operational Security and State Surveillance

The State of Surveillance Explained
The State of Surveillance, a character assassination case study The Five, Nine, and Fourteen Eyes How Far Will Law Enforcement Go?
Anonymity, Pseudonymity, and Operational Security
Crime, Time, and OPSEC
Threat Modeling

Part Three: Considering Operational Security in Social Interactions

The "Just a Man" Philosophy
Public & Private Relations
Trust and Information Disclosure
Degrees of Separation
Sharing is Daring
Sharing is Daring, a Netflix/Skype log correlation case study
Data Poisoning: Disinformation, Misinformation, and Social Engineering
Controlling Disputes and Manipulating Adversaries
Let Them Find Us

Part Four: Considering Operational Security and Your Footprint

A Word on Virtual Private Networks and Tor
Plausible Deniability
Database Breaches & Conscious Account Registration: Understanding Breaches
Database Breaches & Conscious Account Registration: Security Practices
Building a Persona
Persona Contamination: Avoiding Cross-Contamination of Identities
Compartmentalization: Identity Management
Real Identity Safety Considerations

Part Five: Considering Operational Security and Counter-Surveillance

Locational Security
Correlation Attacks
Stealthy Communications (Email, instant messaging, etc.)
Stealthy Communications, privacy and security resources
Leave No Trace

Acknowledgements & Dedications

First and foremost, I have some people to thank. Without them, I wouldn't be where I am today.

To GreySec Hacking Forums, and @cypheractivist for leading the community.

To my mentor @haydnjohnson for being an awesome guy.

To @MalwareJedi for encouraging me to pursue university.

To those who aided me in attending DEF CON and Black Hat USA in 2017: @0x4445565A, @msuiche, @skryking, @peterhuene, @TryCatchHCF, @slyride, Robert Hill, @QFT_, @_eypres, @enkaskal, Xipiter LLC, @KeepBackups, and the others who prefer to remain anonymous.

And to anyone else who has given me a chance.

In a way, the free availability of this book is my way of saying thank you and paying it forward.

It takes a village to raise a child, and you folks all helped me a lot.

Thank you all for your ongoing support.

Part One: The Introduction

Note: You are about to step into the mind of a teenage hacker interested in the crossroads of information security, the human right to privacy, and mass surveillance efforts. This "book" was written during many late nights of my high school senior year in my bedroom, in solidarity, with a naïve passion; only now am I releasing it, years later. This book is not professional, nor is it a properly sourced whitepaper; however, this book is one-of-a-kind, and will further discussion for one particular question that I cannot answer: *where do we draw the line between the right to privacy and national security efforts?* Well, now, I pass the baton to you, other researchers who share this question; I hope you find some answers that you seek to answer this question.

My intention with this writing is not to provide you with a 1-2-3 how-to guide to staying safe online; it is to train my readers into an actively conscious mindset that is a fundamental necessity for surviving in the hacker's realm or in a state of surveillance. It is important that we are able to choose if and when our identity is revealed; Eric Hughes states in *The Cypherpunk's Manifesto*, "privacy is the power to selectively reveal oneself to the world."

If you reveal your real identity to the wrong community or person, they may take the steps necessary to harass, blackmail, and perhaps even unlawfully prosecute in some nations. The target audience consists of privacy advocates, journalists, security enthusiasts, and hackers, but there is a noticeable respect towards the cypherpunk type. People of any background may find this to be a worthwhile and informative read for learning about applying operational security, evading surveillance, and staying safe while surfing the Web. I intentionally wrote this piece to be beginner-friendly and non-technical.

Personal digital security has always been important to me. Everything here is written from my own experience and observations. This writing is authentically original; although, some things are conjectural and anecdotal to a degree, so factcheck where you feel necessary. There have been times where I needed to use the tactics that I will be teaching you about, and there were other times where I had to swear and live by these things to enjoy my Internet experience in a safe manner. The Internet is a dangerous place, especially for those with an interest in information security or anything relating to the hacking "scene."

Again, online hacking communities can be scary, dangerous and hostile places. There are plenty of good and bad people in these communities, and as you probably already know, these people often have malicious intent, even if this is not immediately obvious. You never know who you are talking to online; people can and will lie about their identities, intentions, and actions. They could be social engineering you, and drawing information through elicitation. With this in mind, we must choose what information we share online with great caution. It may even be helpful to lie about your personal information with regularity.

I feel that hackers and many cyber-criminals are strategists in the rawest form; mastered puppeteers, deceitful by nature. You may need to learn how to blend into the "scene" without standing out, and learn to be even more secure than the ones who target you with respect to your personal OPSEC.

An observation that I have made is that many of our youth are also entering the Information Security scene, often overlooked as “script kiddies” and “cyber criminals”. However, I don’t really like to think of most youth as either of the two labels; I believe that we are reaching a new era in technology where youth are learning from curiosity, without a heavy regard for computer laws. Ethical != legal, after all. It is important that ethical youth are not prosecuted in courts, ruining their chances for a successful career at a very young age. The youth hackers of today are the Information Security professionals and leaders of tomorrow.

I want everyone to be safe while pursuing their passion without restriction, whatever that passion may be. Please continue to fight for what you believe in, stay safe, and keep it ethical while you do such. I hope that this reading provides you the foundational knowledge required to operate securely during your cyber experience, whatever your background may be.

Take note that this is not a definitive guide. This research is the result of years of my own personal experiences, opinions, debates, and understanding of the gathered knowledge and resources that I have cited. Personal bias exists within this reading whether I want to admit it or not. Important details may have been overlooked in some areas. Take everything into careful consideration, and think for yourself before acting. You are solely responsible for your own actions.

Additionally, please understand that I am not perfect; inevitably, there will be flaws in this reading. I am an independent researcher and this is an independent project that I have spent a lot of my personal time putting together. Community members have provided me with informal reviews and feedback that I have considered prior to the release of this publication. I have tried my best to take the necessary steps to present this information fairly and accurately while making the reading an enjoyable and educational experience.

With that said, I hope that you enjoy the read.

Part Two: Considering Operational Security and State Surveillance

The State of Surveillance Explained

We will start by looking at the current state of surveillance to acknowledge the difficulty of achieving absolute anonymity and pseudonymity, specifically whilst online. While you may not be a next-level terrorist being targeted by intelligence agencies, I recommend that you understand the breadth of these agencies' surveillance abilities. If an intelligence agency can surveil you, then a dedicated cyber-criminal or skip-tracer may be able to as well; after all, intelligence agencies are really just a collective group of educated people with positions of power, accompanied by powerful computers and a legal system. So, let's get right into it.

The Universal Declaration of Human Rights declares that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." (The Universal Declaration of Human Rights, 1948) In recent years, it has been proven that nearly everyone, everywhere, has indiscriminately had their right to privacy violated on a regular basis.

Ever since 2013, there has been a worldwide debate on the current state of mass surveillance by the government, this is a result of the Snowden Revelations. The Snowden Revelations is a series of once top secret documentation that Edward Snowden stole from the NSA, a vast majority of this documentation discussed violations of the human right to privacy due to the severity of modern day mass surveillance.

Edward Snowden is a whistleblower who had authorized access to top secret government agency documents, belonging to the National Security Agency (NSA). Snowden believed that that the world needed a wake-up call to draw attention to the NSA's unethical mass surveillance practices. The NSA has carried out multiple unconstitutional operations, and consistently violates our human right to privacy. Granted, these things have become common practice amongst intelligence agencies globally. Were you worried about a 1984 dystopian state of surveillance? Well, we are already there and have been since 9/11.

Prior to the NSA file revelations, Snowden worked for the CIA. In Snowden's time with the CIA, he fell witness to corruption within government agencies that violated privacy on a global scale. Snowden decided that he did not have data readily available to him to blow the whistle and have an impact on society that is effective enough to actually initiate change.

Snowden still felt that it is the morally right and ethical thing to blow the whistle on various government agencies for their corrupt surveillance tactics, programs, and strategies. Steering his sights away from the CIA, Snowden found himself working for a new agency: the National Security Agency. He sought employment with a contracting firm in the private sector, Booz Allen Hamilton, that worked closely with the NSA, thus allowing employees to have access to an excessive amount of top secret documentation. This is how he began to collect data that he ultimately ended up sharing when he blew the whistle on the NSA in 2013.

Snowden took an oath to uphold the American constitution, which is what he was doing in a very controversial manner to spark a worldwide debate on privacy and the state of surveillance.

Understanding that the disclosure of this top secret information was illegal, this made Snowden prone to life-long imprisonment and charges for treason and threatening national security. Even though he was not actually trying to commit treason – he states that he loves his nation many times over – let alone threaten his beloved nation's national security, Snowden knew that exposing various corrupt government actions was the right thing to do and had to be done. Again, Snowden took an oath to uphold the American constitution, which is what he was doing in a very controversial manner.

Snowden took the time to collect all of this data, contacted various journalists, specifically Glenn Greenwald and Laura Poitras, through encrypted communications, and worked with said journalists to expose this information to the world. Snowden effectively presented this information to the world, with the help of various journalists, in a manner that ensured optimal social impact that would inspire people all over the world to take a stand against unethical state surveillance. He understood the crimes that he was committing and knew that he was prone to serving jail time. Due to these factors, he remained hushed about his mission until the time was right to reveal his identity as the source of the leaked documentation. Prior to the official public revelations, he explained to Glenn Greenwald that he "is not afraid of what will happen to him. He has accepted that his life will likely be over from him doing this. He is at peace with that. He knows it's the right thing to do." He even went as far as to explain that "he wants to identify himself as the person behind these disclosures. He believes he has an obligation to explain why he is doing this and what he hopes to achieve."

Snowden consistently used, and encouraged others to use, PGP encryption for email and OTR encryption for real-time messaging through XMPP. This allowed him to effectively communicate without unwanted third parties eavesdropping, such as various intelligence gathering agencies, in on his conversations. Encryption basically impairs said third parties from being able to make out what exactly is being communicated, thus causing them to not be able to listen in on conversations where they are not invited. In modern day society, in this state of surveillance, extensive efforts much like Snowden's must be carried out in order to obtain even a shard of one's naturally deserved right to privacy. In fact, encryption and Tor users, specifically those who use PGP, are surveilled by NSA programs such as PRISM and the upstream collection programs such as BLARNEY and FAIRVIEW, just for the sake of identifying those who do care about privacy enough to use encryption. To take it a step further, a lot of this information can be searched through by XKEYSCORE, NSA's "Google" of surveilled information where each webpage is an indiscriminate personal profiling against individuals.

> *"The NSA does not need any specific reason or rationale to invade people's private communications. Their institutional mission is to collect everything,"*

Glenn Greenwald says that "the NSA does not need any specific reason or rationale to invade people's private communications. Their institutional mission is to collect everything," they literally have such a "collect it all, and sort it out later" mentality that an unofficial motto became "collect it all" within the NSA. He goes on to explain that the NSA has shockingly little resistance from governments worldwide, he says that "the sheer scale

of diplomatic surveillance the NSA has practiced is unusual and noteworthy," so it is strange that "country after country, revelations that the NSA was spying on hundreds of millions of their citizens produced little more than muted objections from their political leadership."

William Binney, a mathematician and whistleblower who worked for the NSA prior to 9/11, explains that the NSA "has the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans." Besides Binney, other current and former NSA officials anonymously claimed that in some cases the NSA intentionally "retains the written content of emails sent between citizens within the U.S. and also filters domestic phone calls made with Internet technology." (No Place to Hide, 2014)

To collect such vast quantities of communications, the NSA relies on a multitude of methods; three specific methods, in particular, one includes tapping directly into fiber-optic lines, another includes redirecting messages into NSA repositories when they traverse the US system, and lastly, the agency also relies on Internet companies and telecoms, which indispensably pass on information they have collected about their own customers. (No Place to Hide, 2014)

One of the surveillance programs that is very commonly used within the NSA is called PRISM. The function of PRISM is to tap directly into the central servers of nine leading U.S. Internet companies, extracting audio, and video chats, photographs, emails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post. The nine U.S. Internet companies that data is directly taken from include: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple, services that are very commonly used and mistrusted by subscribers and customers among other people. This is only one of many of the hundreds, if not, thousands of surveillance programs that the NSA is in full control of. (U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, 2013)

> *"Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide."*

Bruce Schneier, the author of *Data and Goliath*, explains, "the powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see but also the prices we are offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide." Both sides will share information with each other, creating an intelligence-sharing network where all accessible intelligence is unethically gathered, traded, sold, and even freely given away.

Much of this information is actually given away voluntary since we are willing to trade our privacy for a transparent lifestyle that can offer us convenience and security. Many people are unhappy when their privacy is violated, and those same individuals can often be the ones who argue that “if you have nothing to hide, then why do you care?” Christopher McCandless, a deceased American adventurer, once said that “many people live within unhappy circumstances and yet will not take the initiative to change their situation because they are conditioned to a life of security, conformity, and conservatism, all of which may appear to give one peace of mind, but in reality nothing is more damaging to the adventurous spirit within a man than a secure future.”

It is not that people do not care about their privacy being violated – not that these intelligence agencies care about you caring about them surveilling you – it is more so that they do not realize that they care. People are willing to store private, sometimes nude photos, in their iCloud, and feel safe doing so since they are offered a sense of security by Apple; however, the same people are very likely to argue that cameras being placed in public bathrooms are a much larger violation of privacy, even if Apple are the ones handling the camera footage and system security. Clearly, these two things are very different, but the point is that people are blinded by an offering of security from large corporations, and do not realize that they truly do care about privacy, just in a different way than one would expect. Though, one thing that many people are not aware of is that the content and service usage on Apple products are free game to the tens of thousands of analysts that work for intelligence agencies such as the National Security Agency, among many many others. The content that they can view is not limited to Apple by any means, but it includes iMessages, phone calls, and even data regarding those private photos we just mentioned that are saved in iCloud; intelligence agencies can potentially view and listen in on your private text messages, phone calls, web browsing history from all devices, photos, and more.

> *Shove a camera in someone's face on the street and they will soon realize the value of privacy, some even putting it above the right to record.*

Although mass surveillance has been an issue for a long time, many of these issues have not been able to come to the general public’s view due to everything being handled in top secret courts, specifically the Foreign Intelligence Surveillance Court (FISC). This court is specially designed to aid the Foreign Intelligence Surveillance Act, thus, everything is done in absolute secrecy. The FISC is an American court, so even when mass surveillance orders are executed on nations foreign to them, many nation’s governments are not notified, thus, other governments are not always even aware of these espionage attacks that invade entire nations right to privacy.

Under the FISA, the NSA receives blanket authorization for global surveillance every year. This blanket authorization authorizes the NSA collectively to surveil everyone in the world indiscriminately; one court's lone annual decision allows an agency to secretly surveil everyone worldwide.

Snowden’s revelations had a significant impact on issues regarding privacy violations and state surveillance; Edward Snowden had, and still has, direct social influence on society that is actively motivating the masses to work collectively with a shared desire to put an end to this unethical, unfair and criminal state surveillance that many government agencies are participating in. These are the effects of the ongoing worldwide debate on the current state of surveillance.

Even when nations' governments are aware of state surveillance, the masses are not always informed; as it was explained before, governments will go to great efforts to keep said surveillance out of the general public's eye. One of Canada's largest surveillance agencies, Canadian Security Intelligence Service (CSIS), will not tell people what information that they have gathered on them. If you formally send them a request to see their file on you, they will comply; however, in their letter's reply to your request, they will only include very limited information from your file, stating that "we, [CSIS], neither confirm nor deny that the records you requested exist," basically explaining in a formal manner that they do not, and will not, give you the full set of records since "it relates to the efforts of Canada towards detecting, preventing or suppressing subversive or hostile activities," even if you have never had any association with anything that would be even remotely considered a threat to Canada's national security.

In a relevant case, the Royal Canadian Mountain Police (RCMP) accessed millions of encrypted messages sent through BlackBerry's BBM service, and managed to decrypt them all, which means that they either hacked BlackBerry or BlackBerry willingly assisted them in decrypting millions of messages, allowing for the viewing of potentially hundreds or thousands of people's personal, private messages that they expect no third-parties to be able to view. This was all an effort to catch a small handful of men. It turns out that the RCMP has had access to the decryption method required to encrypt any messages sent through BlackBerry Messenger in the world since at least 2010. ('Outrageous': RCMP can unlock BlackBerry messages, Dehaas)

Ann Cavoukian, Ontario's former Privacy Commissioner, said the computer code would have allowed police to open not just the "bad guy's" communications, but "yours, mine and anybody's," according to an article from CTV News. On June 9th of 2016, BlackBerry officially admitted to having a special unit that handles government data requests. In this article, BlackBerry officials directly acknowledged and agreed that there are in fact, issues regarding state surveillance in light of the Snowden Revelations. Even though government officials or law enforcement agencies would require a court order or a warrant to carry out said request, Christopher Parsons, a research associate at the University of Toronto's Citizen Lab, explains that he is worried about the secrecy of BlackBerry's process and its potential for abuse. Parsons explains that his "concern would be that there is a lawful order from a corrupt judge, there are countries in the world, unfortunately, where this does happen." All a government would have to do to take advantage of BlackBerry – and many other established companies – to violate the privacy of people, is to either have a corrupt judge or have a government transition to a state of tyranny.

Information gathering agencies around the world are silently forcing a transition to a fully transparent society where everything and everyone loses the ability to express their right to privacy. Many government agencies who are participating in mass surveillance are of nation's that have a democracy. In a democracy, transparency is meant for the government, and the general population, civilians, and citizens maintain their right to privacy; although, government officials seem to be more opaque in terms of transparency than anyone else. Modern governments have the luxury of offering very limited transparency, where they can see everything about a regular civilian in just a few keystrokes and a click of a button. When government agencies have the ability to attend a secret court, execute court orders, and essentially do anything in absolute secrecy with the protection of their own legal system, there is an issue.

Governments have created a surveillance system so sophisticated that it potentially includes hundreds of programs that are solely designed to surveil the masses in different ways. People are surveilled by these programs both inside and outside their legal locational jurisdiction; anyone, anywhere, had the potential to be surveilled at any given moment. Greenwald explains that "the idea that there is a moment when someone can use the Internet or their phone without detection – even for just a few hours while flying – is intolerable to the surveillance agencies" of the world, especially those of the Five Eyes Alliance to the point where a program entitled "Thieving Magpie" was created for the sole purpose of surveilling and intercepting cell phone usage during flights.

What makes a surveillance system effective in controlling human behavior is the knowledge that one's words and actions are susceptible to monitoring.

The scenario that our modern day society is in is becoming increasingly similar to that of which is in the novel 1984. In 1984, people were not necessarily always monitored – or surveilled – at all times; in fact, people had no idea whether or not they were ever actually being monitored at any given time. Although the state did actually possess the capability to watch them at any time, much similar to how the NSA and GCHQ are able to surveil basically anyone networked into the Internet or on their cell phone at any given time. It was the uncertainty and possibility of ubiquitous surveillance that served to keep everyone in line. The point of the matter is made very clear: what makes a surveillance system effective in controlling human behavior is the knowledge that one's words and actions are susceptible to monitoring. (No Place to Hide, 2014)

In "1984", the point was made very clear: you can be monitored at any given moment, so it is crucial for one's personal security to abide the law, and do absolutely nothing to stand out; consistent self-censorship is an absolute must to survive in their society, just as it is starting to be in our own. As a simple analogy puts it, if you are in a public bathroom, you are much more likely to wash your hands when there is someone else in there as opposed to being in absolute privacy; a third-party having the capability of watching and judging you psychologically drives you to act in accordance with the general hygiene standards of society, just as your presence will do the same to them.

If you cannot evade the watchful eyes of a supreme authority, there is no choice but to follow the dictates that authority imposes. If you believe you are always being watched and judged, you are not really a free individual. The deprivation of privacy will crush any temptation to deviate from rules and norms since, after-all, only when we believe that nobody else is watching us do we feel free – safe – to truly experiment, to test boundaries, to explore new ways of thinking and being, to explore what it means to be ourselves. Regardless of how surveillance is used or abused, the limits it imposes on freedom are intrinsic to its existence. (No Place to Hide, 2014)

The possibility of eavesdropping has not only become common knowledge it, in fact, has become a societal expectation.

In a sense, the right to privacy is not the only right that is denied to us due to violations from various governments. Since the government has a psychological influence on the general population to self-censor

things, they are indirectly restricting our rights to both freedoms of expression and free speech. Many people restrict themselves from entering certain search queries into Google and sending messages through social media since they are aware of a third-party being able to intercept their conversation at any given moment. The possibility of eavesdropping being carried out by government officials or law enforcement without a warrant has not only become common knowledge it, in fact, has become a societal expectation.

As Glenn Greenwald said, "privacy is essential to human freedom and happiness for reasons that are rarely discussed but instinctively understood by most people, as evidenced by the lengths to which they go to protect their own [privacy]. A denial of privacy operates to severely restrict one's freedom of choice." Privacy serves as the foundation upon which other human rights are built, and without privacy, one will never truly possess freedom of expression; privacy is something that we, the general population, simply cannot afford to give up. To continue maintaining the little privacy that we have left, and to prevent the situation from worsening, it is crucial that something is done to deter mass surveillance.

It is clear that we are actively living in a state of surveillance. That leaves us with the question: in this state of surveillance, what can we do to achieve a sense of anonymity? Well, achieving absolute anonymity is proving to be very difficult, so instead, consider pseudonymity. We can start by finding a medium where we can achieve pseudonymity to complement our right to privacy while maintaining an identity to express our freedom of speech without (self-)censorship; pseudonymity provides us with a platform to express ourselves openly without the fear of anything affecting our real identity.

To be clear, politically I take a similar stance as Ladar Levison when he said in a piece by The Guardian: "I'm not anti-Government, I'm just pro-freedom." (*NSA Files: Decoded – What the revelations mean for you*, The Guardian) Whether we agree or disagree with Snowden is irrelevant, and there is a lot of controversial debate surrounding these revelations. As privacy and security conscious individuals, it is important that we understand the breadth of surveillance capabilities.

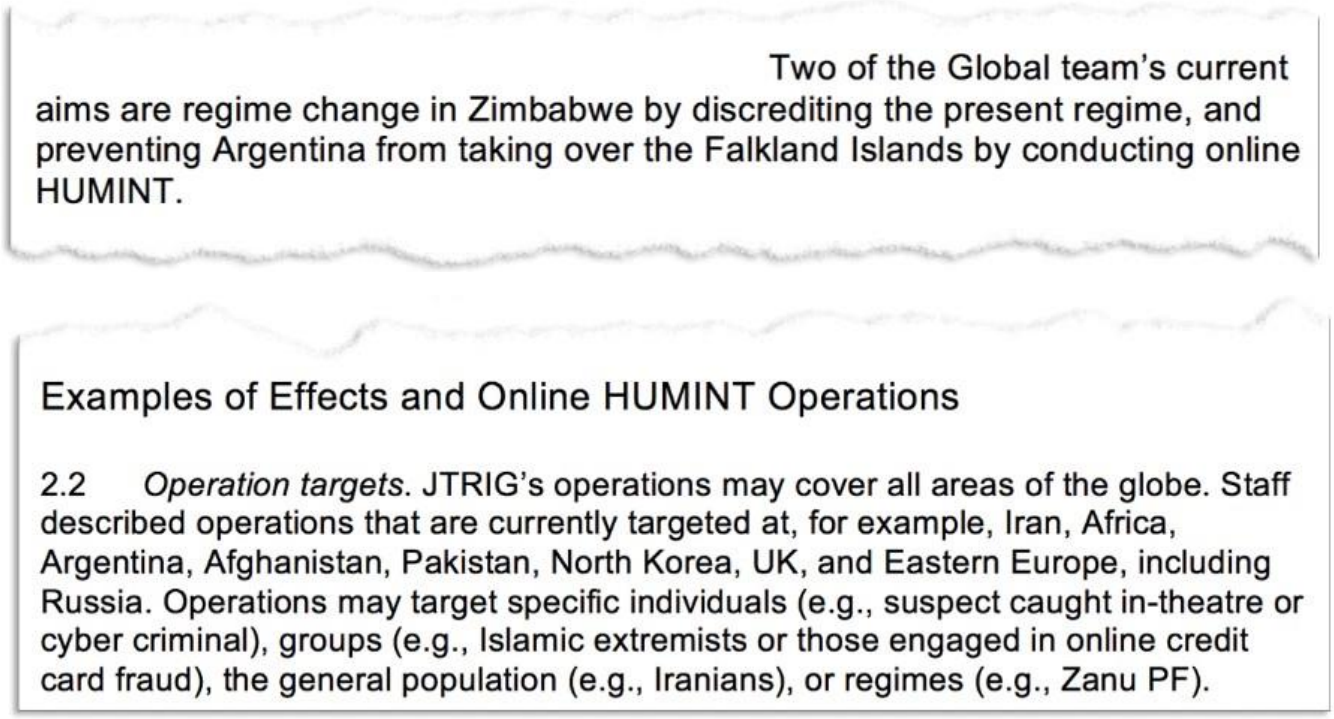
The State of Surveillance, character assassination case study:

Warning: I wrote this years ago, and I understand that many victims have since stepped up since then, likely disbunking this old theory of mine – I wrote this very early on during the Jacob Appelbaum allegations. Please take the following words with a grain of salt, and understand that I was just creating a realistic case study for reader's consideration. If you actually care about this, do your own research.

For some reason or another, a nation-state actor may be interested in silencing an opposition party through discreditation. An intelligence-sponsored state actor group may even be assigned to carry out a politically influenced character assassination with the aim of discrediting core members of the opposition.

There has been discussion of the "4 D's" ruling, developed by the GCHQ and used within their Joint Threat Research Intelligence Group (JTRIG), each of the D's represents: Deny, Disrupt, Degrade, and Deceive. The goal of these 4 D's is to "discredit a target." (*No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Glenn Greenwald)

It is made clear that one of JTRIG's purposes is to carry out character assassination. A leaked document says that "JTRIG's operations may cover all areas of the globe" and "operations may target specific individuals." (*Behavioural Science Support for JTRIG's Effects and Online Operations*, CryptoMe)



Two of the Global team's current aims are regime change in Zimbabwe by discrediting the present regime, and preventing Argentina from taking over the Falkland Islands by conducting online HUMINT.

Examples of Effects and Online HUMINT Operations

2.2 *Operation targets*. JTRIG's operations may cover all areas of the globe. Staff described operations that are currently targeted at, for example, Iran, Africa, Argentina, Afghanistan, Pakistan, North Korea, UK, and Eastern Europe, including Russia. Operations may target specific individuals (e.g., suspect caught in-theatre or cyber criminal), groups (e.g., Islamic extremists or those engaged in online credit card fraud), the general population (e.g., Iranians), or regimes (e.g., Zanu PF).

As we can see in the second example above, specific individuals targeted includes anything from cyber criminals to extremists to even an entire population; in other words, anyone who can be justified as a person-of-interest is subject to becoming an operational target of GCHQ's JTRIG.

Something that we need to remember is that we only know about this due to internal leaks from a whistleblower who had to put their life on the line to share this information with us. With that said, this is one example of a nation state intelligence agency carrying out such operations; we would be ignorant to think that all nations are not partaking in such activities towards the general population, with the entire globe within the scope of their operations.

Let's say that there is a character who has dedicated their life to privacy, anonymity, and security research. As this character does their research, they notice corruption in the functionality of intelligence agencies. Subsequently, they investigate these corrupt acts and work toward sharing this information with the world through publications, presentations, and public speaking. At this point, this character becomes a threatening opposition to intelligence parties since they are aiding in an oppositional movement. It could be in a nation state's interest to execute a character assassination campaign to entirely discredit this individual (mirror

link), and we would be ignorant to look past such *possibilities* (link is a hypothetical theory, not fact – keep an open mind).

Sharing information under a pseudonym enables us to mitigate the impact character assassination has on our real identity, damaging our day-to-day real-life operations. It is good to be aware of what intelligence-oriented adversaries are capable of, and be proactively paranoid.

On that note, it is okay to operate in secrecy under a pseudonym. A pseudonym has the ability to shield us from targeted attacks, such as politically influenced character assassination. In this particular case study, we assume that our adversary is that of a state level. We, as a people, should be able to oppose the state if necessary. Secrecy provides us with the opportunity to cripple an adversary's ability to work against us by starving them of information.

As the Communist Party of South Africa states in one of their works, "There is nothing sinister about using secret methods to help win freedom. Through the ages, the ruling classes have made it as difficult as possible for the oppressed people to gain freedom. The oppressors use the most cruel and sinister methods to stay in power. They use unjust laws to ban, banish, imprison and execute their opponents. They use secret police, soldiers, spies and informers against the people's movements. But the people know how to fight back and how to use secret methods of work." (*How to Master Secret Work*, Communist Party of South Africa)

In the case of day-to-day Internet activities, our adversary is likely more along the lines of a doxer. They may be able to attempt character assassination against our pseudonym, but it is greatly more difficult than if they were to have access to information in our personal lives.

Being capable of working in secrecy not only aids us in outwitting our adversaries, but it provides a layer of protection for our real identity as well. Under a pseudonym, character assassination will become increasingly difficult for our adversary to carry out.

The 5, 9 & 14 Eyes

While we are still thinking about law enforcement and surveillance, I figured that now would be a good time to introduce you to the 5, 9 & 14 eyes. Each eye represents a country involved in an intelligence-sharing group. These "eyes" are allegedly an international intelligence network that assists one another in cases pertaining to state surveillance and intelligence.

The first tier; the original five eyes consist of: USA, UK, Canada, Australia, and New Zealand, they have a massive network of intelligence-sharing called ECHELON.

The second tier; the nine eyes consist of the first tier with the addition of Denmark, France, the Netherlands, and Norway.

The third tier; the fourteen eyes, the third tier, includes all of the previously mentioned countries with the addition of Belgium, Germany, Italy, Spain, and Sweden.

To my understanding, the differences between these three intelligence sharing networks are not distinctly clear. From my understanding, as countries are ranked higher among the eyes (12, 13, 14…), they are less influential, and likely less valuable of an intelligence partner, thus being in a lower intelligence class. For further reading about the "eyes", check out this article on The Daily Dot:
https://www.dailydot.com/layer8/nsa-five-nine-14-41-eyes-alliances-spying/

So, what is the point of all this? If a country is in one of these eyes, they are more likely to share said information with another respective agency in the "eyes" network. For example, if you are using a VPN server that is in Canada, and you perform a malicious attack, causing an issue in another country like the United States, then the United States can request that Canada share the information with them, just as the United States would do in return for Canada since they are both members of the five eyes.

You are going to want to use services that are not based in the "eyes" network, you will want to use offshore services that respect privacy instead. If possible, do not use VPNs, proxies, or anything else in these countries if you are carrying out a questionable operation.

This is just a brief summary of what you need to worry about with the fourteen eyes, in fact, there are even more that we did not discuss. Feel free to research their intelligence-sharing networks more thoroughly if you insist on it, but it only needs to be understood at a high-level glance so you think twice when picking a location to set-up your 1337 cyber fortress like the intelligent hacker you are.

How Far Will Law Enforcement Go?

> "All it takes is a person or persons with enough patience and know-how to pierce anyone's privacy — and, if they choose, to wreak havoc on your finances and destroy your reputation."
> – Adam Penenberg

Truth be told, I do not know how far law enforcement can, or will, go for sure. I am just another security researcher who really likes pseudonyms writing about what I know, but I can try to make some sense of it for you from what I do know, so we will be looking at a few precedents.

Legal investigators, skip tracers, and doxers all share one common characteristic: they are willing to spend an excessive amount of time trying to identify you and interrupt your operations. There is one thing that really distinguishes law enforcement agencies when it comes to cybercrime investigations – they are typically more patient than anyone else when attempting to identify you.

Unlike skip tracers who can get away with breaking the law (to a degree), law enforcement agencies cannot use evidence that they have found in an investigation if it was found in an unconstitutional manner. In other words, they have to follow their own laws whilst investigating you; whereas, you are not required to follow a specific legal procedure when you are taking anti-forensics precautionary measures to combat how law enforcement can go about tracking you.

If law enforcement can find evidence against you, even if they do not know who exactly "you" are, then they will use it in whatever way that is possible to obtain more evidence and information about your identity and activities. This is obvious, but it also worth noting that evidence will be recorded, and it will not go away. You know what they say, once it's on the Internet, it's out there forever. I would imagine that the longer law enforcement is stuck working on a dead-end, the quicker they will be to give up and close your case.

In an article from *Tested* discussing how *the secret service sold fake I.D.'s to catch identity crooks*, it was stated that "the US Government's 'Operation Open Market' resulted in indictments against 55 defendants. More than 125 fake IDs over about five years of activity while going by the username Celtic. Amazingly, the entire scheme started when the government arrested the real Celtic, a Nevada man who got caught shopping at a Whole Foods where he'd previously used a fake credit card.

Law enforcement discovered counterfeiting equipment among his possessions and learned about his online activities. Adams assumed his online identity and even improved Celtic's cred, shipping near-flawless IDs and becoming a trusted seller on Carder.ru."

As you can probably see, in order to maintain your operational security, you are going to want to actively clean up your trails, switch accounts, and constantly cut ties with people and services who pose as a threat to both you personally and your operations. In this example, a L.E. agency took over a real darknet market alias and even acted in the real vendor's place. Evidently, everybody and everything is a threat to your persona's safety.

In another popular precedent, *Silk Road***,** an online black market, and one of the largest modern darknet markets; operated on a hidden service run by Dread Pirate Roberts, the mastermind of the operation. Silk Road users were responsible for a vast amount of illegal drug-related transactions in the few past years. One might wonder how a service like this is operated without being shutdown or people getting caught, and the fact of the matter is that federal agencies don't have a solid hold on hidden services like this, but that is not the point of the matter.

I was reading *The Rise & Fall of Silk Road* and it tells a tale of US government agencies not being able to find anything out about this drug empire – Silk Road – for over a year. Here is a relevant excerpt from the story:

> "DPR, as he was often called, was the proprietor of the site and the visionary leader of its growing community. His relatively frictionless drug market was a serious challenge to law enforcement, who still had no idea who he or she was—or even if DPR was a single person at all. For over a year, agents from the DEA, the FBI, Homeland Security, the IRS, the Secret Service, and US Postal Inspection had been trying to infiltrate the organization's inner circle. This bust of Green and his Chihuahuas in the frozen Utah desert was their first notable success."

Okay, so we have learned that Dread Pirate Roberts makes an effort when it comes to his own personal security, but what's this about this Green character being busted, and Green's bust being considered as a success? I said before that everybody and everything should be considered as a direct threat to you, this includes all personal relations because law enforcement will try to make people turn on you and give up information – Green made a claim that he had [personal relations] with DPR, but luckily for DPR, he did not tell Green much; regardless, the security breach falls within Green's fault, not DPR's, and it was still considered a big first step towards identifying DPR, and infiltrating the Silk Road drug market. The law enforcement will use everything that they can against you, especially your friends. And remember, no one is going to prison for you, so expect them to talk during an interrogation.

Eventually, DPR was arrested due to a variety of things, and The Guardian wrote an article discussing *five stupid things that DPR did to get arrested*. Without further ado, five stupid things DPR did that helped law enforcement see to his arrest:

1. "He boasted about running his international multi-million dollar drugs marketplace on his LinkedIn profile."
2. "He used a real photograph of himself for a fake ID to rent servers to run his international multimillion dollar drugs marketplace."
3. "He asked for advice on coding the secret website for his international multimillion dollar drugs marketplace using his real name."
4. "He sought contacts in courier firms, presumably to work out how to best ship things from his international multi-million dollar drugs marketplace, on Google+ , where his real name, real face and real YouTube profile were visible."

5. “He allegedly paid $80,000 to kill a former employee of his international multimillion dollar drugs marketplace to a man who turned out to be an undercover cop. (*Who are you to decide somebody's death? You are just a man, remember that; we will discuss the “Just a Man” philosophy later in this reading.)*” (*Five stupid things Dread Pirate Roberts did to get arrested*, The Guardian)

In another precedent, Jeremy Hammond – a political activist and computer hacker – was sentenced to 10 years in federal prison for hacking Stratfor, and stealing private information and intelligence. It is claimed that his arrest for the Stratfor case was largely due to him sharing information with Sabu, someone who he thought was his friend, but turned out to be an FBI informant (don't mix this up – an *informant*, not an agent).

According to an article from Alijazeera, “Although [Jeremy Hammond] maintained multiple online screen names to disguise his true identity, Hammond said he became sloppy when he revealed too many personal details about himself to a fellow hacker, which ultimately led to his downfall. He partly blamed his own consumption of weed and acid for allowing his guard to drop.”

By Jeremy allowing himself to share personally identifiable information with Sabu, he got arrested; the personal security issue didn't lie within anything technical, but a personal relation instead.

It is worth knowing that the U.S. government, along with others, are very hard on hackers and cybercrime cases, unfortunately, hackers look at a lot of jail time – arguably more than deserve. It is hard to police the Internet, so the fear-mongering politicians and law enforcement of the United States handles these cases in a very harsh manner to assert fear into the people of our communities. It is important that we as a collective family of communities know what type of unique footprint we are individually leaving behind online; after all, our community does not want to lose another Aaron Swartz.

Sun Tzu once said that “the good fighters of old first put themselves beyond the possibility of defeat, and then waited for an opportunity of defeating the enemy.” You are going to want to assume that this is a very similar mentality of everyone who is trying to locate you when carrying out your operations, and even when you are not. Always be on guard with your enemy, never let your guard down. Assume and act as if you are always subject to targeted surveillance.

The conclusion of the matter is that the law enforcement's efforts to arrest an individual, no matter who it is, will greatly vary based on the severity of an incident, their online persona's criminal background, and access to evidence. In a hacker's arrest, every case is different, no case is the same; everything is circumstantial. It only takes one mistake to get caught.

Anonymity, Pseudonymity, and Operational Security

Anonymity.

Absolute anonymity exists when there is an equal chance of an event (you) being identified among other events (other people) in a set. To be anonymous is to be the same as everyone else in every imaginable way, and vice versa; all participants, or events, in the set must have equally matching characteristics and traits, nothing may be distinguishably different between you and your peers.

To be truly anonymous while actively standing for up for what you believe in is the dream of many hacktivists, human rights activists, and privacy advocates, among many others who face risk for associating their name with their work. We can think of many reasons as to why someone would desire absolute anonymity: to hide from corrupt governments, to avoid prosecution, to maintain a comfortable life of equality, without the stereotypes associated with nationality, ethnicity, and so forth.

> *"You may want to be a ghost, but even Casper has a name; absolute anonymity is not realistic, consider pseudonymity."*

To achieve true anonymity is very difficult. True anonymity means that a single element cannot be distinguished from other elements among a subset of entities. A lot of (meta)data traverses through a network, and systems use unique identifiers such as IP addresses, MAC addresses, among other specifically distinguishable attributes. This information is all vital for the availability of network resources so that you can use a computer in the first place. With that said, you will never achieve true anonymity, only pseudonymity.

Pseudonymity.

In this context, a pseudonym is a masqueraded identity. Using a pseudonym, you are able to create your own identity, and transform it into anything you desire. Operating under a pseudonym will allow you to express your human right to the freedom of speech. In some situations, your pseudonym will be as simple as an XBox gamer-tag, something simple with a less important threat model; in other cases, you may want to totally fabricate an entire identity from scratch. Every pseudonym is created uniquely with respect to the surrounding circumstances. Some people may wish to create multiple identities with different pseudonyms, and compartmentalize to maintain personal online privacy.

The use of pseudonymity is not limited to privacy advocacy and hacktivism! Authors like J.K. Rowling and Violet Blue use pen names – these are pseudonyms, too. Everyone has their own reasoning behind the creation of their persona, and every one of these situations is entirely circumstantial. A common saying of mine when it comes to anything in life, especially identities, is that "*everything is circumstantial*", and your handcrafted persona is too. When developing your pseudonym, it will have to be built around your personal desires, preferences, needs, and end goals.

Operational Security.

How do we assure the confidentiality and integrity of our pseudonym and new persona? There is this big thing called *operational security*. Operational security is a very popular buzzword among security-oriented communities.

Operational security, also called OPSEC, is the art of securing and protecting information within an operational context. Think of OPSEC as our team's defense, it's a defensive mechanism.

If we are aware of an attacker using open-source intelligence against us, or simply attempting to dox us, naturally we would want to protect our information by compartmenting identity information, setting good privacy settings for online accounts, and generally just being cautious about information sharing and communications.

You can execute an operation flawlessly, but that all could mean nothing if someone involved practices poor OPSEC. This could be as simple as someone telling their spouse who they feel they can trust about confidential information, or bragging to an online friend. In other words, loose lips will sink ships.

> *"The opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."*
>
> – Sun Tzu, *The Art of War*

Sun Tzu is saying that it is our own responsibility to secure our operations and day-to-day activities if we don't want to fall victim to an attack. By not doing preparing ourselves for an attack, we are providing the opportunity for a successful attack to our adversaries. Operational security provides us with "the opportunity to secure ourselves" in this regard.

> *"See, the thing is, you only got to fuck up once. Be a little slow, be a little late, just once. And how you ain't gonna never be slow? Never be late? You can't plan through no shit like this, man. It's life."*
>
> – Avon Barksdale, *The Wire*

The fact of the matter is that an attacker only needs to win once, but the defender needs to win every time. To consistently practice "good OPSEC" is easier said than done; in the words of Avon Barksdale, "you only got to fuck up once."

There are some rules that I came across in a video, these are rules that were originally outlined by Nathan House whom I believe was inspired by The Grugq. These rules will vary in importance based on personal circumstances and the operational threat model (we will discuss threat modeling shortly). Throughout this reading, we will be indirectly considering each of these rules. Consider these "Ten OPSEC Rules" listed below.

The "Ten OPSEC Rules":

1. *Always keep your mouth shut;* do not speak unless necessary or beneficial.
2. *Trust no one;* information should be given out on a need-to-know basis only.
3. *Never contaminate identities;* never share anything between aliases.
4. *Be uninteresting;* fly under the radar if possible with respect to your pseudonym.
5. *Be paranoid now;* always plan for how things may go wrong, and have a mitigation plan for later. Maintain proactive paranoia.
6. *Know your limitations;* operate at the level of your abilities, ensure you understand.
7. *Minimize information;* minimize what people can find – if it is not needed, do not keep it.
8. *Be professional;* treat your OPSEC with the seriousness that it deserves.
9. *Employ anti-profiling;* revealing personal information or stories can be used for profiling; remove dangerous information and spread disinformation.
10. *Protect your assets;* use encryption, communicate securely, protect everything, minimize logging.

As we previously discussed, while true anonymity may be unrealistic, we can maintain a pseudonymous identity while applying operational security practices to aid us in meeting our goals.

Crime, Time, and OPSEC

Human nature drives us to have a mutual desire to fulfill our curiosity by creating the products of our inventive imaginations. Unfortunately, legality conflict restricts us, and enforces society's laws upon us through active monitoring and fear-mongering, both offline and online. It is important that we understand may need to assume responsibility for irresponsible or unlawful actions.

Although we may like to respect the law as much as reasonably possible, the threat of punishment restricts us from satisfying our curiosity or bringing our imaginative project to life. Many of these laws are constantly broken due to a conflict of interest, whether it be ethics or a personal decision. Either way, we need to recognize that you will be held accountable for your actions, so regardless of legality, please be ethical and considerate of the impact of your actions.

As the old saying goes: *if you can't do the time, don't do the crime.* If you do the crime and don't want the time, then at least don't speak of the crime. In other words, do not commit the crime if you cannot accept the consequences as reality. When reality hits, it will hit hard – this is why it is critical to be self-aware at all times. You do not want to end up in a similar position as Alexandre Cazes who killed himself after being caught for operating a darknet free market.

If possible, do not break any laws, but historically laws have had to be broken for societal change to be initiated. Some claim that it is acceptable to break unjust laws when necessary, such as Edward Snowden did in regards to global surveillance during recent years; this is an example of a special circumstance where the law had to be broken to cause change to occur.

Example #1: Edward Snowden and the NSA revelations

Let's recap for a moment: Edward Snowden is a whistleblower who had authorized access to top-secret government agency documents, specifically documents belonging to the National Security Agency (NSA). Snowden believed that that the world should know that the NSA is actively performing state surveillance in a manner that is extremely violating and invasive to our international human right to privacy. Due to a of conflict of interest in terms of ethics, Snowden moved forward with revelations.

Prior to the NSA file revelations, Snowden worked for the CIA. In Snowden's time with the CIA, he fell witness to corruption within government agencies that also violated privacy on a global scale. Snowden decided that he did not have data readily available to him to blow the whistle and have an impact on society that is effective enough to actually initiate change.

Snowden still felt that it is the morally right and ethical thing to blow the whistle on various government agencies for their corrupt surveillance tactics, programs, and strategies. Steering his sights away from the CIA, he set and locked his sights on a new target: the National Security Agency. He sought employment with a contracting firm in the private sector, Booz Allen Hamilton, that worked closely with the NSA, thus allowing

employees to have access to an excessive amount of top secret documentation. This is how he began to collect data that he ultimately ended up sharing when he blew the whistle on the NSA in 2013.

Snowden's revelations had a significant impact on issues regarding privacy violations and state surveillance; Edward Snowden had, and still has, direct social influence on society that is actively motivating the masses to work collectively with a shared desire to put an end to this unethical, unfair and criminal state surveillance that many government agencies are participating in. His initial goal was to spark a worldwide discussion of surveillance and privacy, and he succeeded in doing so by breaking *a few* laws in the process, consequently dubbing him as a traitor to the nation-state. Whether you disagree with Snowden's intent is irrelevant, the point of the matter is that we should be able to act upon a conflict of interest, especially when it involves a breach of human rights.

Snowden understood that disclosing this top secret information was illegal and made him prone to life-long imprisonment and charges for treason and threatening national security. Even though he was not actually trying to commit treason – he states that he loves his nation many times over – let alone threaten his beloved nation's national security, Snowden knew that exposing various corrupt government actions was the right thing to do and had to be done.

Snowden took the time to collect all of this data, contacted various journalists through encrypted communications, and worked with said journalists to expose this information to the world. Snowden effectively presented this information to the world, with the help of various journalists, in a manner that ensured optimal social impact that would inspire people all over the world to take a stand against unethical state surveillance. He understood the crimes that he was committing and knew that he was prone to serving jail time. Due to these factors, he remained discreet about his mission until the time was right to reveal his identity as the source of the leaked documentation. Prior to the official public revelations, he explained to Glenn Greenwald that he "is not afraid of what will happen to him. He has accepted that his life will likely be over from him doing this. He is at peace with that. He knows it's the right thing to do." He even went as far as to explain that "he wants to identify himself as the person behind these disclosures. He believes he has an obligation to explain why he is doing this and what he hopes to achieve."

Edward Snowden does not speak much of his own operational security, but here is some of what we do know, he: chose to reveal the revelations specifically in Hong Kong, secured his communications using encryption, claimed to have go on a recovery trip to Hong Kong to clear up a mental condition, checked into a hotel under his own name, used his own credit card, encouraged others to practice operational security to maintain anonymity on both ends, and his threat-model only required short-lived anonymity until he was targeted by the United States government.

Hong Kong is a city within China, and simply being in China ensured his physical safety from the United States, specifically in the form of extradition. It would be more difficult for the US to operate against him in China when compared to other countries; Hong Kong would be more willing to resist the pressure that the US would put on them than other nations. He felt that Hong Kong had the best mix of both security and political strength

among his options. Following thorough consideration, Snowden decided that Hong Kong is the best place to stay while he leaked the documents; great consideration was put into choosing Hong Kong as the place to reveal his prepared revelations.

In mid-May of 2013, Snowden had requested a few weeks off of work, under the claim that he needed to go somewhere to receive treatment for his newfound epilepsy condition. He never told his girlfriend about his mission nor his intentions, let alone where he was going; he did not tell anyone where he was going for the sake of both their security following the repercussions of his actions and his own. It is best that fewer people knew what he was doing; otherwise, they would likely receive harassment from the government following his revelations.

Once he arrived in Hong Kong, to avoid suspicion, he checked into Mira Hotel using his own name and credit card. He explained that "he knew that his movements would ultimately be scrutinized by the government, the media, and virtually everyone else. He wanted to prevent any claim that he was some type of foreign agent, which would be easier to make had he spent this period in hiding. He had set out to demonstrate, he said, that his movements could be accounted for, there was no conspiracy, and he was acting alone. To the Hong Kong and Chinese authorities, he looked like a normal businessman, not someone skulking off the grid." (No Place to Hide, Glenn Greenwald)

Snowden consistently used, and encouraged others to use, PGP encryption for email and OTR encryption for real-time messaging through XMPP. This allowed him to effectively communicate without unwanted third parties eavesdropping, such as various intelligence gathering agencies, in on his conversations. Encryption basically impairs said third parties from being able to make out what exactly is being communicated, thus causing them to not be able to listen in on conversations where they are not invited.

The point of the matter is that rather than blatantly publish all of this information alone and anonymously, Snowden took the time to plan and strategize the best ways to effectively spark a global outcry for the halt of unethical state surveillance. In Snowden's own words, he "[wanted] to spark a worldwide debate about privacy, Internet freedom and the dangers of state surveillance". As a result of his actions, he is not currently imprisoned but living under the protection of Vladimir Putin in Russia, and the people of the world are working together to defend and protect him.

As of 2017, Snowden has still avoided extradition from the United States of America, and he is supposedly living comfortably within Russia's borders.

Example #2: David "Caliconnect" Burchard

In another case study, we are going to look at David Ryan Burchard, a 38 year old man from Merced, California, who was arrested and accused of distributing marijuana and cocaine throughout the United States using several darknet markets including the Silk Road, Agora, Abraxas, and AlphaBay under the moniker "Caliconnect". Federal authorities estimate that the total worth of every transaction made by
Caliconnect is $1.43 million. (*Timeline: Arrest Of The Darknet Market Vendor 'Caliconnect*', Fuzzy)

For starters, David sold millions of dollars of Bitcoin to one currency exchanger alone, this is what initially made him get noticed by an agent from Homeland Security (HSI), causing the initial investigation case to be opened on him.

That isn't all though, the name that he sold drugs on darknet markets under, he trademarked it; David Ryan Burachard trademarked the handle that he used for dealing drugs, "Caliconnect", in his own name.

Next, he contaminated his persona by declaring himself as the same seller from other darknet markets such as Silk Road, Silk Road 2.0, and the Black Market Reloaded, on Agora. He discussed the crimes that he has committed, thus indirectly confessing to committing a series of other crimes that otherwise may not have been traced back to him in the court of law let alone in law enforcement investigations. No defence lawyer will have an easy time saving him from that blatant confession.

David had actually printed his trademarked name on to clothing, claiming that it was his "Caliconnect" is his clothing brand. He even had the confidence to try to claim that he sold clothing and sold absolutely no drugs whatsoever.

To top it off, an article explains that "computer forensics on Burchard's computer and storage devices revealed a lot of incriminating evidence. Caliconnect's logo that was used on AlphaBay was found along. Decrypted PGP messages were provided by the computer forensics agent. Bruchard's PGP password was "asshole209" which was apparently reused since it was a password given to the computer forensics agent by Larsen which was obtained from subpoenaed records. One of the 49 PGP messages retrieved was the same one caliconnect4life sent to
Megiddo. Burchard's bitcoin wallet was found as well." (*Timeline: Arrest Of The Darknet Market Vendor 'Caliconnect'*, Fuzzy)

Caliconnect is a prime example of someone with a very poorly executed operation lacking security in several aspects, it may be reasonable to go as far as saying that he did not practice any operational security at all. We can clearly see the difference in operational security application between Caliconnect and Edward Snowden. Snowden planned for his crime, thus he did not "do time"; Caliconnect did not plan for his crime, thus "did time." Applying operational security appropriately can save you from jail time, especially if practiced correctly.

As you can see, sometimes these operational security guidelines may need to be altered to assist you, this entirely depends on your circumstances. Your actions could potentially create both a positive social influence and also attract unwanted attention from law enforcement at a state, federal, and international level. It is entirely your own responsibility to make wise decisions at this point; ensure that you are understanding what you are saying, or sharing, at an intimate level to make the wisest decision. If one does not first consider the potential repercussions that their actions could cause, they are just asking to be imprisoned due to their blatant carelessness.

If we make a point of displaying exemplary operational security in this manner, it will inspire others to act more responsibly since they will consider the potentially significant impact their actions could have prior to unwisely committing crimes. By making people consider this basic operational security, we are essentially preventing the dangerous practice of bad operational security, and increasing the practice of commendable operational security procedures. By considering your actions before acting them out, you make a decision better than the one you have made otherwise.

Threat Modeling

> *"Threat modeling is a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized – all from a hypothetical attacker's point of view." - Wikipedia*

Every strategy should have a threat model, whether it is a network threat model or a theft prevention program at a mall. Upon creating a threat model suited to your circumstances, it is good practice to consistently rethink your threat model to identify new or previously unknown threats to our identity or operation.

In terms of identities, we should be aware of threats that reveal our identity as false in some respect. A threat is anything that can lead to our identity being exposed as false or the leaking of personally identifiable information. Common threats for identity exposure typically includes persona contamination, correlation attacks, and "loose lips", among others.

Persona contamination is the cross-contamination of personally identifiable information across identities. An example of this includes using your real name in a uniquely identifiable user name.

A correlation attack is the correlation of data in an effort to prove that you performed a subset of activities. An example of this would include being caught for launching a network attack from a McDonald's and getting caught due to the correlation of network traffic and camera footage.

"Loose lips sink ships" is a common-folk saying, heavily used during World War II to promote operational security practices. Many people reveal their identities through a breach of confidentiality in common conversation. An example of this would be to brag about a *1337* hack you performed, and having that information spread as a result, leading up to your arrest. Think of this as a self-binding non-disclosure agreement in the interest of not sharing information that will breach your identity or operation's confidentiality.

Since the focus here is on threat modeling, let's consider a specific type of threat model: the OPSEC model. I am going to include content from my own article on AlienVault's website for this section since there is no point in re-explaining it in different words. (*Managing Pseudonyms with Compartmentalization: Identity Management of Personas*, CryptoCypher)

The OPSEC Model

An OPSEC model – a set of standard procedures to ensure operational success – should be established for maintaining each individual persona. The goal of our OPSEC model is to mitigate the risk of the operation being jeopardized while maintaining operational capabilities, it is the bridge that allows us to rationally execute operations with success. This OPSEC model will describe the rules and conditions to be followed while using that persona, this protocol will also outline how a persona will react to various situations. The established protocols of our OPSEC model should always be followed.

Risk Perspectives for Your OPSEC Model

B3RN3D suggests in his Perspectives of OPSEC Models article that there are a few risk perspectives that we should consider for our OPSEC Model: adversary-centric, asset-centric, and software-centric. These perspectives will aid us in determining what perspective to consider for our OPSEC model.

Adversary-Centric OPSEC

"In these types of plans, we're focused on what an attacker or adversary can do to us; who is coming after you, what they can do, and how you can defend. An adversary-centric policy has the advantage of being much easier to create and document because many people already think this way. It's very simple to come up with a list of adversaries that have the potential to affect what's important to you. The down-side of this approach is that you need to know your adversaries. In the case of the NSA "revelations", many were shocked to find out that a nation-state had the type of capabilities that were disclosed. Prior to this, not many were able to mitigate themselves from these types of threats because they simply didn't know or fully appreciate an adversary of this nature." (*Perspectives of OPSEC Models*, B3RN3D)

Asset-Centric OPSEC

"This approach focuses on designing mitigations around your assets – the things you value the most. If, for example, your asset is your ability to privately communicate on the Internet, you're going to do everything you can to ensure no-one can affect this. You're not focused on specific adversaries per se in this approach, but you are doing everything in your power to protect yourself. Maybe you're buying a VPN service or using a botnet or Tor for all communications. Maybe you've decided that you're going to try out one of the new decentralized messaging systems (ie. XMPP protocol for instant messaging, protected with OTR encryption) as a way of keeping yourself secure." (*Perspectives of OPSEC Models*, B3RN3D)

Operation-Centric OPSEC

"This approach […] lends itself nicely to compartmentalization if you're managing multiple identities across multiple operations. An operation, in this case, could be an identity, a research project, a regular activity or whatever, that may require specific operational security measures. An operation-centric OPSEC plan may sound recursive to you, but the gist is that your plans are focused on your specific operation and that operation alone. The main difference between this and an assetcentric approach is that it is designed to have drastically different and compartmentalized procedures allowing for scalability without letting one operation interfere with another." (*Perspectives of OPSEC Models*, B3RN3D)

When developing your OPSEC model, it will be beneficial to determine who your adversaries are, what assets you need to protect, and how to manage the operation in the most secure manner possible. By considering these three perspectives, your operational security will be strengthened.

So, Who Needs an OPSEC Model?

Everyone needs to follow rules of some sort to perform their daily operations safely, but the need for an OPSEC model depends on the operational circumstances. There are a limitless number of possibilities for the various different models that could be created, again, respective to the operational circumstances.

Ross Ulbricht, better known as Dread Pirate Roberts, is an ex-darknet marketplace operator convicted of founding and running the Silk Road. Determining the OPSEC model for a darknet marketplace operator is difficult since there is a vast variety of metrics that must be considered: law enforcement investigators, state-level adversaries, targeted blackmail and extortion, and even assassination attempts.

A darknet marketplace operator would require dedicated compartmentalization, the capability of plausible deniability, regular anti-forensic action, a cover-up career, effective money laundering, and strong self-discipline to avoid sharing stories in real life. Additionally, they would require a strong understanding of how to maintain cyber anonymity through cryptocurrency, secure messaging, understanding of metadata, cryptography, and much more. This is an example of an extremely delicate OPSEC model, to say the least.

To read more about who should be using a threat model, consider this article.

Corporate OPSEC Models in InfoSec

Realistically, not everyone is a darknet marketplace operator, but we often see OPSEC models used in our very own workplaces; we can think of defensive security policies, rules, and guidelines as pieces of a greater corporate OPSEC model.

InfoSec professionals often say that the human factor is the weakest link in security. By developing rules and defensive security policies in the workplace, various types of social engineering attacks can be prevented. Everyone involved with the security industry would benefit by enforcing defensive security in the workplace. Incorporating defensive security, like an OPSEC model, would help maintain corporate reputation by preventing data exfiltration. By using a corporate level OPSEC model, many physical security threats can be mitigated in the workplace.

How Do I Measure my OPSEC Model?

B3RN3D introduced a model to define levels of OPSEC for identities. The model has five levels, ranging from Level 0 to Level 4; 0 being the least protection necessary, and 4 being the highest. We will use this model for identifying levels of necessary OPSEC; however, this model is not to be considered a trusted method of evaluation since every operation is unique and should be treated as such. Always take the time to tailor your OPSEC to satisfy the operation's circumstances.

B3RN3D's OPSEC Level Model:

- "Level 0 – No protections. You don't care about privacy and are not concerned with other people attributing your online activities to yourself.

- Level 1 – Minimal: You are concerned about privacy, but choose simple, minimalist tactics to protect yourself. For example, you are using a VPN service for everyday browsing, but being caught is inconsequential.

- Level 2 – Medium: You are concerned with your privacy and take action to ensure that you are safe. It is likely that if someone finds out what you are doing, you'll have to pay a price, but it is not a life-and-death situation. For example, journalists working with a source use the TAILS LiveCD.

- Level 3 – High: Those users that are likely to be targeted, and likely to have heavy consequences if caught. They have done everything in their power to maintain their pseudonymity, but still, try to lead some semblance of a personal life.

- Level 4 – Extreme: These are reserved for those people doing high risk activities where the result of an adversary outing you is a matter of life and death. You're prepared to forgo personal relationships, worldly goods, and just about anything to maintain your anonymity."

If you are stuck between two levels, do not fret. Remember that these are only models of a theoretical hierarchy, we can adjust them according to the operational circumstances. There is no single correct way to develop your threat model, so feel free to be creative.

Part Three: Considering Operational Security in Social Interactions

The “Just a Man” Philosophy

You are just a man (or woman…).

People will act irrationally; subsequently, they may make poor decisions. Irrationality is no excuse when you are in a position where your power and influence cause external impact. Power and influence can cause the development of an egoistic personality, leading to the addiction to self-importance and a desire for vanity. Ego and vanity will often lead to poor operational and information security practices, in turn, causing an operation to fall apart or backfire with consequence.

Emotions and the desire to feel powerful can sometimes get in the way of logical decision-making, and influence us to do irrational things. We often forget that we are only people. If you ever think that you are taking on more than you can probably handle, please stop and remember that you are only human. You are just a man, you are just a woman; you are only human. Nobody really cares about who you are online, so stop acting like it.

It may be fun to boast your ego, living like you are in the fast lane, but it is dangerous for operational security practices. When I have become egoistic in the past, and it has happened, I have learned to correct myself by reminding myself that I am *just a man*.

“you’re just a man” - Marcus Aurelius

There once was a man named Marcus Aurelius, a Roman Emperor from 161 to 180. He ruled with Lucius Verus, as co-emperor, from 161 until Verus' death in 169. Aurelius was the last of the Five Good Emperors, and he is also considered to be one of the most important Stoic philosophers.

Aurelius would regularly walk through the streets with citizens bowing down to him, offering him complimenting words of praise, and even more than this at times. Despite this, he never wanted the praise make him lose sight of his goals. So, what did he do? He hired a servant to follow him through the streets and whisper to him "you're just a man, you're just a man…" every time someone bowed, got on their knee, or praised him in some way or another.

Aurelius said that people should "wrestle to be the man philosophy wished to make you," and Abraham Lincoln said that "the best way to test a man's character is to give him power.”

Test your power honourably and always maintain a level head when decisionmaking in any situation. Control your urges, have respect for both yourself and others, and maintain your moral values. Do not submit to temptations prior to thinking about the associated risks. It is critical we are able to control egoistic habits at any given time when in a role with power and influence. By realizing this and acting responsibly, we subsequently become better leaders as well as operational security practitioners.

Public & Private Relations

Plan for social situations, whether they are public or private; always think ahead, and always consider your words carefully. Speak every word with tact.

Relationships are all around us, regardless of identity. We have family, friends, adversaries, allies, partners, and so forth. Subsequently, we must always be prepared to know how to handle our relations, whether these relations are *public* or *private.*

One can investigate how they would like to approach a social engagement by considering the two mentioned relations categories: *public* and *personal*. A public social relation pertains to communications between two parties that are in public setting. A private social relation pertains to communications between two parties that are outside public setting.

"Loose lips sink ships," this is something that we have all heard at one time or another; the information that you choose to share with others can be detrimental to the success or failure of an operation. If you speak too much, you may reveal sensitive information that will negatively influence your operation. If you speak too little, your operation may fail, as you were too afraid to line up the information to carry out the operation in the first place.

How you should handle a situation is depicted by the circumstances of the operation; with that said, *everything is circumstantial. N*o matter how many guides you may read, you should be prepared to make a split-second decision that compliments your OPSEC model in a social situation.

Public Relations

Managing public relations is essentially the practice of handling communications between two parties in a publicly viewable social setting. Public relations includes discussions held on social media, public forums, public IRC channels, and so forth. I would even go as far as to say that any communications that are plaintext and unencrypted during transit (ie. HTTP, FTP, etc.) should be considered public due to adversaries analyzing our network traffic. If the relation is not one-on-one or an isolated group discussion, then it is likely a public relation.

When engaging in public relations, one will want to limit the information they are providing to websites like Twitter, Facebook, public forum websites, or messaging platforms available to the public (ie. IRC, XMPP chat rooms, etc.). Whenever you share something online, post the information on a need-to-know basis; ask yourself, "Does a Twitter follower really need to know my date of birth, mother's maiden name, or who my best friends are? Do they need to know that I just planted my first rootkit?" Your followers do not actually need to know anything about you, and they will not think that you are anything special – refer back to the "Just a Man" section of this reading, if you must. You may make adjustments as necessary for your operational goals and your respective identity's OPSEC model.

Consider yourself public enemy number one at all times, your adversary is always on the lookout. Limit the information that people have access to, make appropriate judgment calls with respect to the operation's circumstances.

Case study: Facebook taunts send another "catch me if you can" crook to jail

To summarize the story, a 40-year-old UK fugitive and convicted drug dealer from Merseyside, Steven Johnson, used alias Facebook profiles with fake names to share pictures of his life whilst on the run, making a statement in his posts, directed at law enforcement – "catch me if you can. […] You will never find me!" This game did not last for long.

Unfortunately for this UK fugitive, his attempted cat-and-mouse game had a short-life. Law enforcement had used basic investigative methods with the help of Facebook metadata. The tactics that police use to track these drug dealers down are similar to those that may be used against a hacker. Metadata is data about data that is stored everywhere, and even worse, it exposes you, so limit the spread of metadata however you can.

Hackers, doxers, skip-tracers, and law enforcement alike use similar tactics to track targets of interest. Metadata is your enemy; everything contains metadata, whether it be photos, network packets, videos, or PDF files.

Photos that you share may contain Exchangeable Image File (EXIF) data that reveals information such as camera speculations, date and time of photography, as well as GPS information that reveals where the photo was taken. Many image hosts and social media giants strip EXIF data from images but remember that metadata is always a risk to you. You can modify EXIF data using tools such as ExifTool. To remove all EXIF data with ExifTool on a Linux platform, try this command in the directory containing the target image file: *exiftool -all= image.jpg*

Excessively sharing personally identifiable information (PII) is something that our society has become accustomed to doing due to the changing state of the Internet, specifically the growing popularity of social media. Every second of every day, people all over the world are placing their PII in databases (name, date of birth, usernames, email addresses, etc.) We live in the era of Big Data – people and services analyze information shared on the Internet constantly. As a result, our information is sold, traded, shared, and targeted; some people will act with malicious intent, others will aim to profit financially from your data, and others may want just want to hoard your data. In some cases, doxers will gather PII, typically via social media, and publish doxes on their targets.

To find an example of a dox, using this string in Google's search engine: *site:pastebin.com "dox"*

My point with this public relations stuff is simple: do not share personally identifiable information on the Internet where you can help it. Be aware of how your information is being shared. If you have bad OPSEC on social media and whatnot, you will have bad results!

> *"Basic rule: Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember when in Rome, do as Romans do. Don't try to be a smart ass. Feds are many, Anonymous is Legion, but you are only one. Heroes only exist in comic books keep that in mind! There are no old heroes; there are only young heroes and dead heroes"*
>
> - The Über Secret Handbook

Private Relations

A private relation refers to a relationship between individual people or private groups of friends. Private relationships can be very broad and complex. Mutual experiences, personal emotions, and other complex circumstances will inevitably have an influence on your private relationships because as much as we would like to practice flawless OPSEC, everyone still needs a friend to talk to.

You will run into like-minded people on the Internet. It is totally okay to make friends, acquire acquaintances, and develop your network, but it is not okay to share any personally identifiable information with those who do not need to know it, especially if they are from a security-oriented community. Friends turn to foes. Generosity turns into greed. Partnerships turn into betrayal. So share information on a need-to-know basis where possible.

Be careful with whom you associate yourself with. It would be a shame if your entire cover were blown due to a friend with "loose lips." This is especially applicable if they are guilty of wrong-doing because when push comes to shove, no one is willing to go to jail for you.

A hacking community is not a place for your personal feelings. Once you join the community, it becomes your second life, not your first. Friends are for real life, not for hacking communities. Quite frankly, if your social life is lacking to the point where you have no one to talk to about your problems, either make change or take it to another non-security community. Sharing feelings and life stories is a daring engagement. Also, when I say "hacking communities", I am not just referring to InfoSec Twitter. In contrast to other communities, InfoSec Twitter is extremely kind and non-malicious.

A bit of personal advice here: I have been around hackers all throughout my teenage years, I have friends who do security research, and I have met cyber criminals of various degrees. Some remained loyal, but in the end, they all left, or I left, and you will too. Hacker relationships are only temporary. Everybody leaves the "hacking scene" eventually, and many people change aliases without warning frequently, so do not allow others to carry your information or secrets with them for when they do eventually disappear. It is common to re-encounter old contacts without even realizing it. Do not expect them to warn you when they disappear either – hackers are not your friends. Friendship in hacking communities is only temporary. You never truly know who you are speaking to in a community of hackers.

Unfortunately, we need to maintain private relations in order to maintain positive mental health, and you may run into a mental burnout from going overkill on your own OPSEC model; this is where

compartmentalization comes into practice for security-minded folks. Compartmentalizing your aliases can help you manage your private relations. We will discuss compartmentalization and OPSEC burnout later, in a dedicated section of this reading.

Trust and Information Disclosure

We will often times find ourselves gaging how much we trust someone prior to disclosing information to them. This doesn't only apply to operations, but this also applies to our personal lives. If we trust someone, we are more likely to rely on them to keep a secret; our will to share information increases if we trust someone. It seems like common sense, right? I agree. However, we should still run through some considerations for the sake of this reading.

Trust, what is it?

Merriam-Webster says that *trust* is:

> *"(1) : a charge or duty imposed in faith or confidence or as a condition of some relationship*
>
> *(2) : something committed or entrusted to one to be used or cared for in the interest of another."*

In the context of this reading, trust is the condition that people use to determine whether they can rely on someone to perform a task or withhold a secret. There is a truster and a trustee. Determining whether we trust someone to keep a secret or perform a task can be daunting because we often cannot be positive of the outcome. In some situations, we must make decisions based on trust, which could either end well or very poorly.

In an article by Dr. Marty Nemko, he discusses a game he played with a close friend, where they agreed to take turns answering one another's questions with complete honesty. He asked her, "Do you ever have any negative thoughts about me?" Instead of responding with something simple, she honestly said "I'm jealous of you so I sometimes think of hurting you." The simple story goes to show that even our close friends could potentially act out against us, regardless of us *trusting* them. (*How Can You Tell Who to Trust?*, Marty Nemko)

How do I know who to trust?

Honestly, it's hard to know who you can truly trust, and I'm not exactly a psychologist. I read some articles about the psychology of trust, and most seem to say to look for a comfortable balance between *warmth* and *competence* in people. In other words, someone can be seen as *trustworthy* if they are socially friendly enough to feel comfortable talking with them, and competent enough to be consider a credible person. If you strike someone as friendly, competent, reliable, consistent, and honest then they will probably be more likely to trust you.

The fact of the matter is that we won't always know who to trust. Like we mentioned in Nemko's "honesty game," even those who we trust may potentially stab us in the back.

In one article, Thomas Koulopoulos discusses "5 Way to Tell If Someone is Untrustworthy," which seem logical:

1. “They lie to themselves

2. They project behaviors on you that are clearly not ones you are exhibiting

3. They breach confidentiality

4. They show a lack of empathy

5. Their emotional state is volatile, and they have a pattern of inconsistency and fickleness in their decisions” (*5 Ways to Tell If Someone Is Untrustworthy*, Thomas Koulopoulos)

When it comes down to it, you will have to decide who you trust and why you trust them on a case-by-case basis.

How do people disclose information?

As we said, deciding on whether or not we trust someone can be challenging. The fact of the matter is that relationships and operational security simply do not blend together well at all. People are the weakest link of security, and the more people that we involve in – or let have knowledge of - an operation, things can become messy.

A *trusted* individual could be interrogated or extorted for the personal information of their co-operatives. Also, an individual could be *falsely trusted* with information, and they disclose it elsewhere which will draw in negative or unwanted attention. These are just two hypothetical situations to consider.

With these considerations in mind, B3RN3D asked the question “How do you determine if you should share a secret with another person and build a relationship with that person at the risk of compromising your campaign?” To answer this question, we analyze their “Analyzing Trust and Secret Disclosure” article, but I will also include a few direct excerpts.

It is important that we identify what information we share, and how much of this information we decide to share. Here are the three tactics that B3RN3D proposes for information disclosure:

1. **Trusted Disclosure**

   - Analyze the relationship, consider the risk of sharing the information, and the potential reward if you do share.

   - “Option 1, trusted disclosure is where you analyze the relationship with the other person, look at the risk involved in disclosing, and the potential reward that exists if you do share. This is what some may call “normal” in terms of relationships. You decide that you will disclose a secret to a trusted person and expect that the trusted person does not use this information against you. If for example, you know that the other party has worthwhile knowledge related to your secret, the reward may

outweigh the risk that the disclosure is used to exploit you." (*Analyzing Trust and Secret Disclosure*, B3RN3D)

2. Plausibly Deniable Disclosure

◦ Hint that you may have a secret but leave room for plausible deniability.

◦ "In option 2, plausibly deniable disclosure, you hint that you might have a secret but you can still plausibly deny that the secret exists. There is less analysis of risk vs reward or analysis of the trust of the person so you'll often hear people leak this in public. "I might know something about X but I can't tell you". If you go to DEFCON, you will hear this just about every day." (*Analyzing Trust and Secret Disclosure*, B3RN3D)

◦ "This is the most common tactic with people missing social contact/relationships and let their ego get in the way. This either means that the secret being kept is not that risky of a secret, or the person is not disciplined enough to follow OPSEC. In either case, frowned upon in terms of OPSEC." (*Analyzing Trust and Secret Disclosure*, B3RN3D)

3. Zero Knowledge

◦ No disclosure, but maintain a zero knowledge relationship with that party.

◦ "The last option is not a disclosure at all but maintains a zero knowledge relationship going forward. In terms of OPSEC, you can consider this a firewall rule that blocks all by default. In this scenario you get no reward, no commonality in the relationship, and no benefit besides the fact that you can keep in your pocket that you have a secret in-depth knowledge of a subject that may be of interest to the subject. Because remember, knowledge is power and knowledge of someone's knowledge is a power you may not want to concede." (*Analyzing Trust and Secret Disclosure*, B3RN3D)

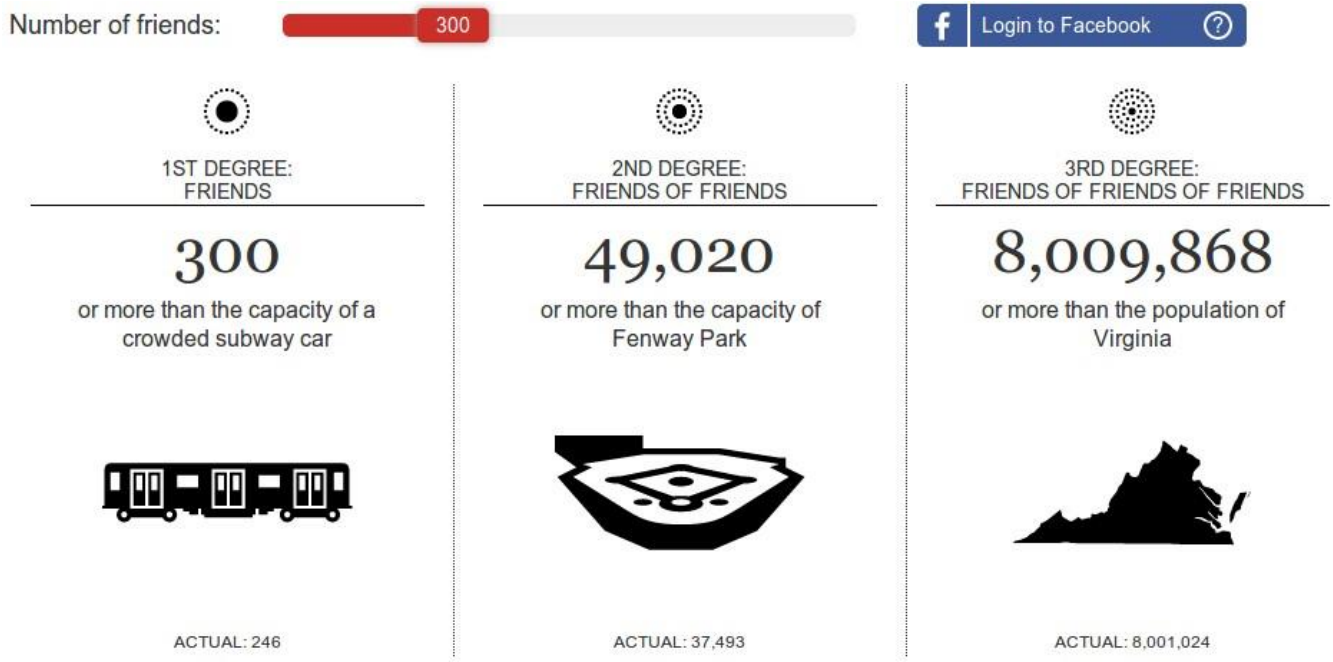
The approach you decide to take may vary. Many hackers take the Zero Knowledge approach, and many of us naturally use the Plausibly Deniable solution by default. Tread carefully around regularly practicing Trusted Disclosure.

Degrees of Separation

In this section, we will consider the theory of the *six degrees of separation*, and we will be putting a special focus on the first two degrees of this six-degree network. The idea of the six degrees of separation is that everyone in the world is connected to every other person through a "friend of a friend of a friend" model, such that everyone is six, or less, steps away from everyone else in existence.

At some point, you will be connected with the entire human population by the sixth degree of separation. Each immediate connection of yours being the first degree, then any connection of theirs is the second degree, and so forth, this is the theory of the six degrees of separation.

In an excerpt from The Guardian's *NSA Files: Decoded* project, an interactive scale is used to provide an example of how many people are subject to N.S.A. surveillance efforts. The excerpt explains that "you don't need to be talking to a terror suspect to have your communications data analysed by the N.S.A. The agency is allowed to travel "three hops" from its targets – who could be people who talk to people who talk to people who talk to you." (*Three degrees of separation: breaking down the NSA's 'hops' surveillance method*, The Guardian)



Screenshot from The Guardian's 'degrees of separation' scale, where n = 300.

In the 1990's the U.S. National Security Agency developed a project called "ThinThread," ThinThread was discontinued after the attacks that took place on
September 11, 2001, and replaced by a similar project called the Trailblazer, and Trailblazer has now been replaced with Turbulence, and this may have been changed since then.

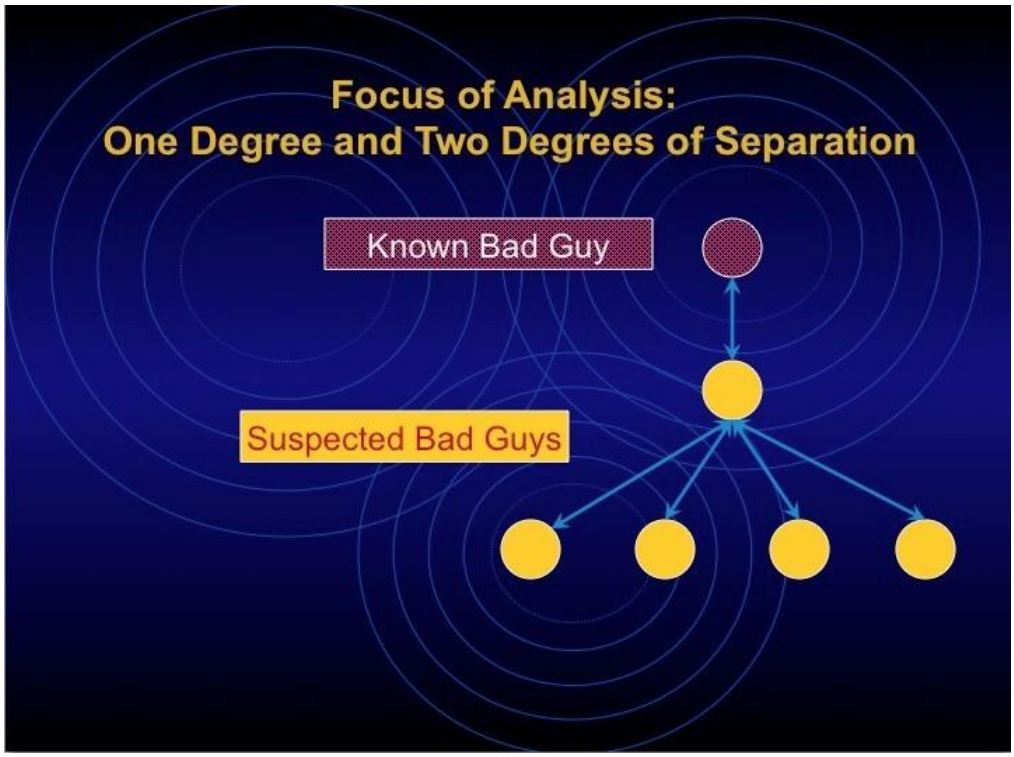
ThinThread had an emphasized focus on automating wiretapping and intelligence analysis against the general public. According to zdnet, "the project included legal restrictions and privacy filters that would encrypt and scramble USrelated communications to prevent illegal and warrantless domestic snooping."

Tim Shorrock, a writer on U.S. national security and intelligence, explained how ThinThread operated in three distinct phases:

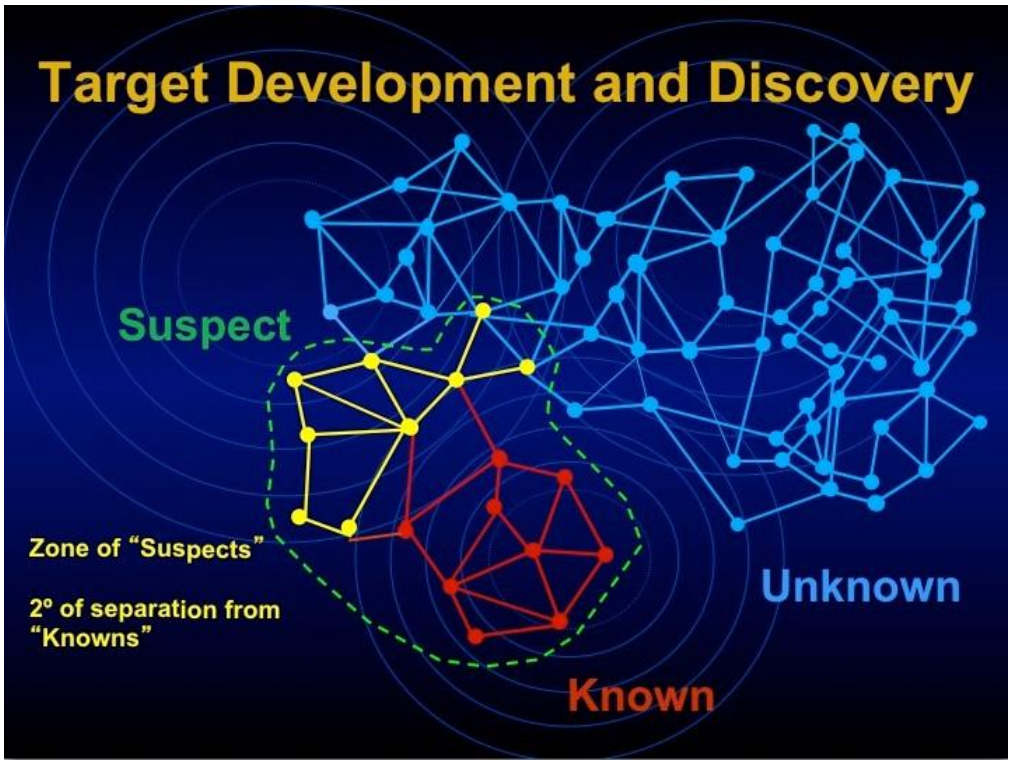
1. *"First phase:* ThinThread intercepts all call conversation, email and internet traffic on a network and automatically focus analysis on specific targets using specific patterns of information."
2. *"Second phase:* ThinThread automatically anonymize the collected data so the identities stayed hidden "until there was sufficient evidence to obtain a warrant."
3. *"Third phase:* ThinThread uses the raw data to create graphs showing relationships and patterns that could tell analysts which targets they should look at and which calls should be eavesdropped on." (*ThinThread spy system secretly tested on New Zealand population*, Pierluigi Paganini)

In the third phase, ThinThread generates graphs to reveal relationships between suspects connected to known "bad guys" and others. The N.S.A. would monitor these relationships and build a network of suspects based on the first two degrees of separation. In other words, by interacting with a known "bad guy," you are automatically listed as a suspect, and so is anyone that you communicate with, including your friends and family. In this scenario, everyone involved within the first three degrees of separation is promptly placed on the N.S.A.'s radar and become subject to a form of targeted surveillance. This "justified surveillance" will occur despite being morally unjust, considering that it is an invasion of the human right to privacy.

Two slides regarding ThinThread were shared by N.S.A. whistleblower, William Binney, in his ThinThread presentation, to visualize the degrees of separation with respect to ThinThread. (*NSA Whistleblower William Binney Private Presentation/Q&A on Snowden Files/THINTHREAD*, William Binney)



Anyone in contact with a "known bad guy" is a "suspect bad guy."



Dividing up the "degrees" into "Suspect", "Known", and "Unknown" groupings.

Despite the ThinThread project has been discontinued, there are still similar and even more sophisticated programs that are actively being used by intelligence agencies all across the globe to monitor your activities.

This is one of many live surveillance projects. There are many more of its kind, including the surveillance efforts of nation-states all around the world. We would be foolish to assume that only America does this.

You can try to prevent yourself from getting caught up in one of these networks by carefully choosing who you communicate with, and carefully planning out your communications. You cannot be tracked as easily if you avoid unique identification in the first place. Avoid communicating with people-of-interest who are open about what they do by mocking the police, attacking the government, harassing and threatening people, and Tweeting their little heart away about the box they just popped or the account they just 'jacked.

Your friends can reveal a lot about you, so if you speak to people of interest to national security, then I am willing to bet that you are labeled as a suspect, too. And again, remember that no one is going to jail for you, so be prepared for those connections to throw you under the bus if they are ever interrogated. We must carefully evaluate who we choose to include in our social network.

Sharing is Daring

While we are on the topic of surveillance, consider the following: have you ever watched a show on Netflix and talked to your friends about said show? By sharing this information with your friend, you are creating a negative impact on your OPSEC, this is because you are revealing identifiable preferences, and you are also sharing your digital footprint with a service; you are setting yourself up to be hit by a correlation attack (discussed later), and your real identity may be discovered through trivial investigative techniques. This example may be extreme, but the point stands: sharing is daring, regardless of the subject at hand.

You may be wondering: what is so bad about talking about my favourite TV show on Netflix? Every time you watch a TV show or movie on Netflix, logs will be kept to identify what you watch, how long you watch it for, and when you watched it. You will be profiled based on the genres you typically watch to make personalized recommendations. These logs are a part of the metadata that Netflix keeps attached to your account. Netflix, like many other services, will learn patterns that are unique to you, thus creating a distinguishable footprint unique to only you. Law enforcement or another type of adversary could now progressively use this data to narrow down the list of suspects, and eventually cause issues for you later in time.

If you are talking to another person and you mention that the new season of Breaking Bad was released on Netflix, followed by a discussion regarding you loving it so far, this implies that you are watching this TV show on Netflix. As silly as it may sounds, an adversary with access to these logs could include them to further differentiate potential suspects. This also ties into *correlation attacks*, which will be discussed in more detail later.

Sharing is Daring, a case study: *tracking a hacker via Netflix and Skype logs*

Okay, so take it a step further now: there is an open investigation on you and your activities, and a conversation was had over a targeted Skype account. Assume that the law enforcement knows about the Skype account that belongs to you, so they get a warrant to seize the account, and retrieve all of the logs. Within these chat logs, you tell the tale of you watching Breaking Bad on Netflix to your hacker friend. Now the law enforcement knows what show you watch, and that you have an account on
Netflix.

The law enforcement now contacts Netflix with a court order, or a warrant, requesting that they share what Netflix accounts have watched certain episodes of
Breaking Bad in a set timeframe, and Netflix obeys this court order. Now the law enforcement has a list of Netflix accounts, and they know that one of these accounts belongs to you. Breaking Bad is a popular option, so while it may provide a large sample set of users, obscuring your identity even further, what if you were talking about an unpopular show that only 27 other people watched in that day? That still leaves 27 suspects.

What if the investigator pursuing you has another piece of information, specifically your time zone? Perhaps they made an educated guess of your time zone based on your online activity at certain times. The investigator could then determine which of those 27 users are in your time zone. The result of this brings them down to 13 suspects in this hypothetical; you are one of 13 suspects. Let us assume you are a hacker and because of that, you are more likely to work in I.T. So, how many of those 13 remaining suspects work in a computer-related profession – two? Now we are getting pretty close to home since law enforcement just determined that you are likely to be one of two people.

"… always be self-aware…"

Yes, I know this all sounds silly; however, hypotheticals like this one are considerably realistic in intelligence, and they must be considered to maintain OPSEC. To uphold your OPSEC, you must always be fully aware of what information and what metadata you are sharing. You must always be self-aware of the personalized footprint that you are creating for yourself across multiple platforms and services.

Sharing personal information is dangerous! Do not share anything personal, and if you really must then learn to communicate it all through disinformation, misinformation, social engineering and just flat-out fibbing at a convincing level. We can start by understanding what methods we can use to influence and manipulate others, respectively.

Disinformation: *Intentionally lying.* Disinformation is false information that is shared with the intent of being perceived as true to the receiving party.

Misinformation: *Unintentionally lying.* Misinformation is false information that we may unintentionally share. We may want to have others spread misinformation for us; this can be done by planting disinformation.

Social engineering: *Influencing others to act in a desired manner.* Social engineering is the art of influencing or manipulating others to act upon your desires through carefully planned interactions. Social engineers often use elicitation to gain information.

Combine all of these factors into one, and let's call it *data poisoning*.

Data Poisoning:

Disinformation, Misinformation, and Social Engineering

Data poisoning is the act of spreading false, misleading information about yourself, hence the poisoning of the data. Your goal when data poisoning is to be so convincing about your claims that no one reading any of the disinformation will believe otherwise. You want your lies – disinformation – to be consistent as if they all connect together; when your attacker is connecting the dots of your identity, the disinformation must be convincingly real. I personally feel that data poisoning is the basis of any fabricated identity; this web of disinformation will become your new online identity.

Is your name Jack Daniels? Well, it is Captain Morgan to everyone else now. Did you just buy a new car for 5000 USD? Well, you just bought it for 6500 AUD now. Do you enjoy a nice glass of wine on the odd night? Well, now the only thing that you need to be sipping is orange juice on a warm day… To anyone who is not you, at least... I think you get the point. Of course, this information still needs to align with your identity.

Before you are ready to engage in data poisoning, you will need to do a bit of aggravating work and research to determine the structure of your new identity. You will need to look into what accounts and information will surround your identity (eg. Facebook, Twitter, ask.fm, GreySec, etc.), and create a unique username, email(s), and password(s) around such identity. You will also need to determine characteristics such as your identity's geographic location, national currency, occupation, hobbies, attitude, stylometry, local time-zone, and so forth.

This identity, like any other, will have an attitude and style. You will need to look into stylometry, considering that everyone's writing is uniquely identifiable. Create an appearance, and how it will communicate with others too (will you be friendly? standoffish?). You can create the appearance by finding someone who is unpopular on a social media website and using said photos, and consider tailoring any EXIF data prior to use. I recommend using photos of someone you don't know. You need to decide on every little bit of information you will be sharing for the sake of consistent disinformation; of course, this may vary based on your end-goal.

Your task is far from complete there. What about when you are chatting in realtime? When you are on IRC, Skype, Facebook Messenger, XMPP, or any instant messaging platform, it can be very easy to slip up. You must ensure that you are always following your schedule and that you do not speak about anything personally identifiable to you. If the person you are speaking to is convinced that you work a 9-5 job every day then you probably do not want to be talking to them during said hours within your persona's time zone, unless it makes sense to be (Remote work? IT? Selfemployed?).

Naturally, people speak about events taking place in real-time. When given the chance, incorporate small events that influence your target into associating traits with your persona that otherwise would not be related to you. For example, if it is cold outside, talk about how hot it is. If your persona enjoys soccer, talk about a soccer tournament that is presently taking place. Again, assuring that the disinformation is sensible.

As DIzzIE says, the aim must always be to present the illusion of transparency, an "I have got nothing to hide" hologram. (*HOW TO LIE TO PEOPLE: ACHIEVING ANONYMITY THROUGH DISINFORMATION AND DATA POISONING*, DIzzIE) You should want this disinformation and poisoned data to piece together so nicely that they just cannot believe otherwise. Again, to do this, you will need to be consistent with your disinformation and make sure that it makes sense. Once you decide on your persona's characteristics, you cannot start change many of these traits; speak sensibly. An example of this is that you cannot say that you are 18, but born in 1989 on May 2nd, and then change your age and date of birth a week later. Your adversary will notice these careless mistakes.

Attacks on your personal identity can happen when you least expect it. There are many reasons why someone may choose to attack you. Someone may be social engineering you with an underlying motive of acquiring information about you and your family, or they may be looking for something to blackmail you with, and the possibilities are truly limitless. These attacks will often happen before you even realize it or expect it. These personalized attacks occur every single day in online communities, it is more common than you may like to believe. Attacks on your identity are generally preventable with data poisoning, at least in the context of online communities.

Preventing these personalized attacks is achieved by simply not sharing our personal information; instead, we share disinformation: fabricated information about a fabricated identity. This will allow you to speak freely without the fear of having your character attacked by a malicious party. If the attacker does not have an opening to discover our identity, then there should be no problem. Additionally, our adversary may become convinced that we are someone else entirely if we apply data poisoning effectively.

When it comes to operational security in terms of identity, it is critical that the defender wins every single time; the attacker only needs to win once to march their path to victory. Do not let your guard down and maintain consistency with your disinformation. Consistency is critical for any operation, especially when data poisoning.

Why would you want to lie about all of this? As I said before, attackers could use any of this information to single you out in a crowd, even if that crowd contains 7 billion people or billions of indexed pages from Google that your information is sitting on. People will go out of their way to single you out, be prepared for when they do look into you; secure your persona in every aspect – every little nook and cranny – possible. Who knows, maybe someone even contracted a doxer or private investigator to target you.

For further reading, I would suggest checking out DIzzIE's paper on *Achieving Anonymity Through Disinformation and Data Poisoning*.

On a conclusive note, it is important that your targets do not know that they are being lied to. If it is clear that you do not trust them, then they will show distrust in return. I will leave you on that note with a relevant memorandum.

Memorandum on the Effects of Atomic Bomb
To: Harry S. Truman, September 11, 1945

"The chief lesson I have learned in a long life is that the only way you can make a man trustworthy is to trust him; and the surest way to make him untrustworthy is to distrust him and show your distrust."

Henry Stimson, Secretary of War

Controlling Disputes and Manipulating Adversaries

Dispute and conflict are a part of human nature. Malicious individuals often have a bloodlust for conflict, and an eye for profitable disputes, especially on the dark side of the Internet. Due to this malicious atmosphere, we should always ensure that we are in control of our own personally identifiable information, and sometimes it is necessary to manipulate the adversary to have them act how we would like them to act.

Before you find your way into a dispute, you may want to ensure that you have already won the battle beforehand through careful planning of strategic operations. You will need to be capable of manipulating your adversary. It may benefit your operation to have a solid persona, back-story, and you will want to know exactly what you are doing. You will need to discipline yourself at the same time since a solid story and persona alone will not lead you to victory during your dispute, you must be convincing. Although, this is entirely circumstantial based on your operational situation.

Sun Tzu once said that “victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win. Thus it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory.” The same concept applies here, a puppet does not control a puppeteer; however, a puppeteer does control puppets. The puppeteer is manipulative and will pull the appropriate strings to make it’s puppet act out in the desired manner. If you can manipulate your adversary, then you can also call the shots on wins and losses with increased ease. You want to be the puppeteer, not the puppet; you are one or the other, you decide.

In the past, we have discussed limiting information exposure. To limit information exposure means to control who and what can see which specific information, and when and where they see it, too. If your enemy is limited to only this information then you already know every possible point of attack that they have. With an intimate understanding of by what means your information can be accessed, it becomes easier to identify their movements and mislead them through data poisoning.

Although, this will most efficiently succeed if your enemy does not know that they are a puppet caught in your strings, being manipulated to do your biddings. You may want to “appear weak when you are strong, and strong when you are weak.” (Sun Tzu), and it would be in your interest to achieve the supreme art of war by subduing the enemy without fighting in the first place. Your enemies are puppets, you are the puppeteer – take control of those puppets, and manipulate them into going in a direction that is most convenient for you, but try not to allow them to know that you are manipulating them.

Allow yourself time to prepare prior to the dispute, and when an Internet dispute happens, you normally will have time. This gives you the upper-hand, the ability to speak and act with patience and awareness, control your ego, and plan for your adversary’s manipulation carefully. If you apply these three principles, you can plan to win your dispute well in advance.

You are a puppeteer, a controller, and manipulator. Information can be controlled, just as puppets are. The opportunity to take control of a dispute and manipulate your enemy is always there.

This section has been very philosophical, so take my words into consideration with a grain of salt.

Let Them Find Us

The concept of Let Them Find Us (LTFU) is simple and self-explanatory; if we hide in plain sight to avoid standing out. People will often forget to fact-check, and we can fly under the radar with no questions asked if we take advantage of this while data poisoning. People often assume that your claimed identity is who you are without fact-checking, so if you drop the whole "anonymous" masquerade, then you can get by without people thinking to fact-check your identity. If your identity is solid, you will not need to worry about this, but it is generally best to fly under the radar where possible just in case you slipped up somewhere. This LTFU concept is security through obscurity in a sense.

"Curiosity killed the cat," so avoid making people curious

If we flaunt around wearing an Anonymous (Guy Fawkes) mask, people will wonder, "just exactly who is it behind the mask?", they become curious – this is what we don't want. Like we just said, "curiosity killed the cat," it is important that we avoid making people curious about your identity unless it somehow benefits your operational goals. It would be better if they did not have to be suspicious of you in the first place. If you do all this, people will not think to look for more; we are mitigating the need to search for us.

You do not want potential attackers to know that you are trying to hide your real identity. You want them to believe the fake disinformation – your data poisoning – that you have intentionally put out there already. The information must look real upon investigation; for optimal effectiveness, it must look real so the potential investigator feels no need to investigate in the first place. They must believe the lies over anything else at all costs. Do not give them any reason to let them think anything that you do not want them to think, stick to your guns, and keep your ego on the down-low while influencing them to move according to your operation's plan.

After all, you are *just another man* amongst a crowd, so do not mess it up by sticking out unless necessary. In most situations, it is probably better if people just think of you as a harmless person, not a malicious hacker or a secret espionage spy, even if you are one; of course, this is not the case for those who need to have a highprofile persona. Again, everything is circumstantial with your identity.

Assuming that you applied the data poisoning techniques, the information should already be convincingly real. Act with the personality that you have given your persona, stay consistent, and never data poisoning – *make it all convincingly real, and don't stand out by looking as if you have something to hide*.

Part Four: Considering Operational Security and Your Footprint

A Word on Virtual Private Networks and Tor

Virtual Private Networks (VPN)

> "A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network." (*Cisco Secure Virtual Private Network*, 2002)

A VPN can be thought of as a message-relay service that exists between you and the destination specified in your packet headers to protect your privacy from external people and networks; this service is in the middle of all of your data exchanges. Remember that this man-in-the-middle can still intercept, monitor, log, and inject malicious packets or code into your session, so it is important that we are able to trust our VPN provider.

When it comes to selecting your VPN provider, it all comes down to who you feel you can *trust*, and who can back their claims of *strong encryption* and *no logging,* and *reliable delivery*, as much as possible. Any 17 year-old kid on HackForums can set-up an OpenVPN instance on a DigitalOcean droplet and call it a "reliable, log-free, encrypted, offshore" VPN service, but do you really trust this "service"? Do your own research regarding which VPN you are going to use, and choose carefully. It will also be worth your time to find a provider that operates offshore for the sake of being protected by a different set of laws that respect privacy and are outside of American jurisdiction.

Another thing is that you will want to avoid are free VPN services; there is a saying that goes something along the lines of "if you are not paying for the product, you are the product," and this especially applies to VPNs. In an analysis of 283 VPNoriented services offered to Android devices on the Google Play store, it was found that there are heavy presences of third-party user tracking and access to sensitive Android permissions, malware presence in 38% of the applications, heavy concentration of American network infrastructure (NSA will likely have access to this data), and there are countless weak points that leave users vulnerable to various modes of traffic interception. (*An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps*, 2016)

VPN Recommendations: CryptoStorm and Mullvad

My go-to VPN providers are CryptoStorm and Mullvad, both claim to be reliable VPN services that encrypt their traffic, hold no logs, and promising reliable delivery.

CryptoStorm takes it a step further by claiming to be committed to their "Privacy Seppuku Pledge," a pledge promising to shut down their services prior to participating in surveillance efforts, or as described in their words:

> *"The Privacy Seppuku pledge is simple: if a company is served with a secret order to become a real-time participant in ongoing, blanket, secret surveillance of its customers... it will say no. Just say no. And it will*

shut down its operations, rather than have them infiltrated by spies and used surreptitiously to spread the NSA's global spook malware further. You can't force a company to do something if there's no company there to do it." (Privacy Seppuku Pledge & Wall of Honour, CryptoStorm)

Again, the VPN that you decide to use all comes down to whose word and infrastructure you truly feel that you can comfortably trust. As of right now, there is no single rock-solid VPN solution despite what any person or provider claims. Please, for your own sake, do research and choose wisely.

Also, remember that VPNs are for privacy – not anonymity.

No VPN provider is willing to go to prison for you.

Why is it a bad idea to host my own VPN?

- Reason #1: Personally identifiable information and financial information is typically required for account registration which is tied to your server's host.
- Reason #2: Correlating traffic to independent clients is more challenging when multiple users are connected to the same server node, opposed to a single user. This leaves some potential for plausible deniability.
- Reason #3: You'll probably fail at configuring something on your server. It is literally your VPN providers job to know how to handle your data safely, both before and during transit.

Tor Project – What is it?

Put simply, *Tor is a service that allows you to browse the Internet anonymously,* but sometimes adversaries manage to identify Tor users, so we need to be extra careful by keeping the software as up-to-date as possible.

The Tor Project offers free software and an open network that is used to help defend against traffic analysis from external entities, whether that entity is a statesponsored adversary, an intelligence agency, or a cyber-criminal snooping on your traffic.

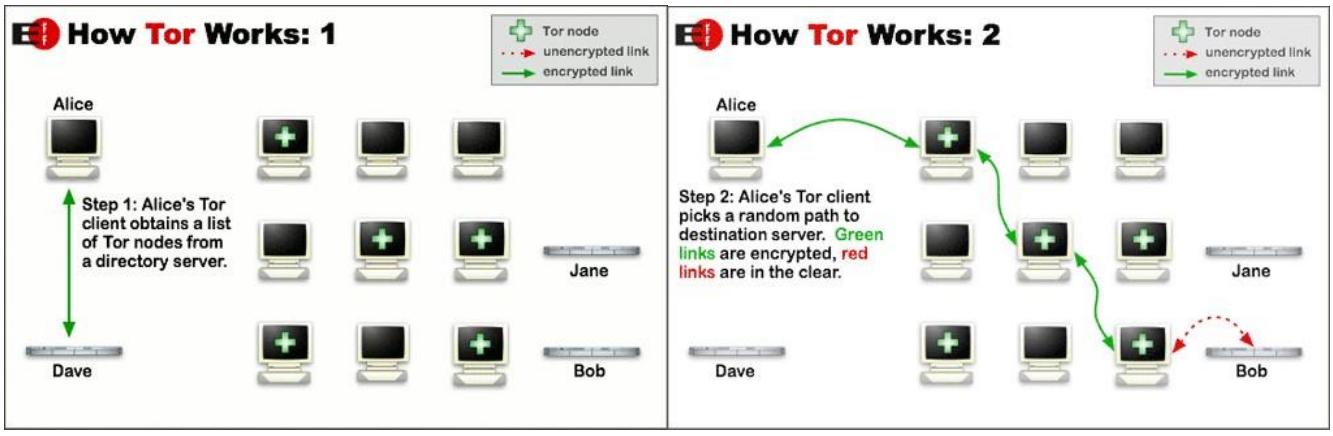
Tor conceals users' identities from their online activity by separating the systems' identification and routing processes using their own implementation of onion routing. Onion routing encrypts communications and bounces them through a network of relay nodes, that are hosted by volunteers all around the world, and exits through an exit node. The exit node is the only node that is revealed to a host on your destination network.

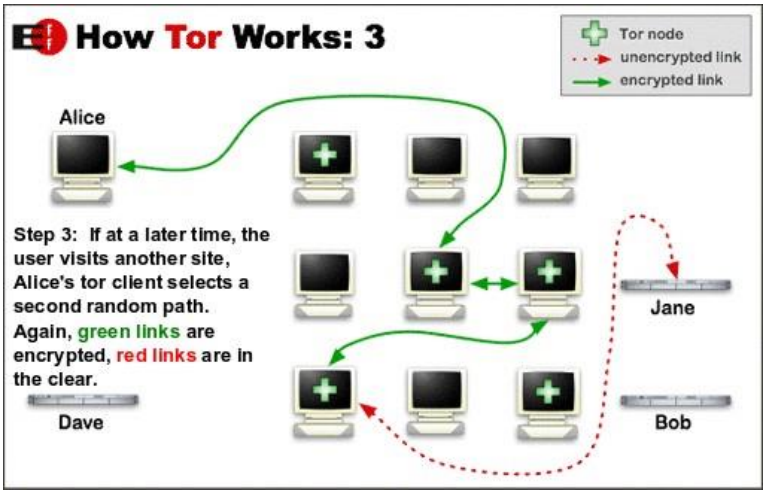
Cool – now we know that Tor can make our data bounce through a network. So, what exactly is unique about the Tor network that makes it good enough to protect ourselves from the bad guys, and just how does this network make us anonymous?

We are able to maintain a sense of anonymity in the Tor network due to both the source and destination addresses are not stored in plaintext in any node while routing through the network. If anyone is listening in on our communications, they are going to have a very difficult time trying to identify both ends of the connection.

It is worth noting that we cannot maintain absolute anonymity whilst online just by using Tor alone. Achieving absolute anonymity is impossible, there are new attack vectors found every day, and this includes attack vectors that may be used against the Tor network to identify users like ourselves; these attacks are carried out both by regular people, and attacks against Tor are also popular among intelligence agencies. In fact, intelligence agencies like the FBI value these attack vectors to the point where they would rather drop a child porn case than give up a Tor exploit (Newman, 2017). You will also hear stories about law enforcement setting up honeypot nodes for the sake of gathering information on Tor users, so keep that in mind too.

To solidify our understanding of the Tor network, take a look at these graphs provided by the EFF to visualize what exactly is happening between the source and destination host:





For the extra paranoid folks, and the technologically curious, you may be interested in The Grugq's *Personal Onion Router To Assure Liberty* (P.O.R.T.A.L.) project. This project encompasses configuring a router to ensure all traffic that goes through the router is routed through the Tor network. Configuring this router may be ideal for preventing information leakage, but is not entirely necessary.

> "PORTAL is a project that aims to keep people out of jail. It is a dedicated hardware device (a router) which forces all internet traffic to be sent over the Tor network. This significantly increases the odds of using Tor effectively, and reduces the potential to make fatal mistakes." – The Grugq

You may become a target of surveillance simply for using the Tor network or a VPN. Authoritative figures seem to have a complex about people ensuring their privacy using these technologies, and unfairly labels them as suspect due to this prejudice. You should take use Tor, but remember that nothing will ever guarantee your absolute anonymity – not the Tor network, nor a VPN. ***So, stay frosty.***

Plausible Deniability

Plausible deniability is the condition that allows you to plausibly deny something. An example of plausible deniability would be if someone was telling you about the idea of an operation but not enough to actually discuss it in detail, they intentionally limit the information you possess to control plausible deniability. In this example, a subject is deliberately made unaware of said truth to benefit or shield the subject from any responsibility associated with the knowledge of such truth. This can apply to protection from authority when being probed in an interrogation. Of course, plausible deniability is not just limiting information exposure, but it also includes creating a threat model that allows you to comfortably deny specific accusations, even if said accusations are true.

When you are detained, investigated, and interrogated, you will need to be able to rely on a set of pre-determined plans to determine your future since you can no longer rely on yourself to make any changes to the operation at hand. These predetermined plans are where plausible deniability comes into play. You want to be able to rely on plausible deniability since you cannot do anything else.

Police and lawyers are required to follow a legal system. Even if the police do not believe you, and they feel that they know that you did something, you can continue to deny involvement under certain conditions. Until the investigation proves you to be a liar, you can freely deny whatever you please within reason. If law enforcement fails to provide valid evidence acceptable to a judge's standards in the courts, then that evidence will often be dropped from the case, and it cannot be picked up again – you are free to go at this point for that case in particular; however, criminals and hackers do not have to follow this system.

If the criminals targeting you discover your identity, there is not much that you can do to convince them that their investigative results are false. They will likely think that you are trying to social engineer your way out of the bad-looking situation at hand. These lies can easily aggravate them too, thus worsening your situation. It is advisable that you choose your words very, very carefully when speaking to your attacker; depending on the circumstances, it may be better if you say nothing at all.

We need to remember that plausible deniability can only work if we have conditions in place to support what we are denying. For example, if you are trialed for a hacking incident, and you shared different, unrelated hacking experiences through message logs that have been brought forward by a snitch, then you will have a hard time denying these other accusations. If there is nothing behind these logs, and they were stored in a text file, off-server, no paper-trail, then you may be able to plausibly deny the accusations; there is a chance that the evidence will be dropped due to invalidity since the courts do not know if the snitch tampered with the data at hand.

If said logs are server-side and accessible outside the snitch's local host, things probably will not look too good for you. So, keep your nose clean and you will be fine, or at least keep your activities out of the public eye, news, and especially social media that ties back to any identity of yours; claiming any illicit responsibility is a bad, bad, bad thing for your operational security, just do not do it.

Something worth noting is that plausible deniability does not always work, especially when you decide to eliminate any evidence that you already have. Just because it is no longer existent, does not mean that the judge cannot believe that it was once there before you destroyed it. What I am talking about is called "spoliation of evidence in the court room."

According to the *Wikipedia*, "The spoliation of evidence is the intentional, reckless, or negligent withholding, hiding, altering, fabricating, or destroying of evidence relevant to a legal proceeding. Spoliation has two possible consequences: in jurisdictions where it is the (intentional) act is criminal by statute, it may result in fines and incarceration (if convicted in a separate criminal proceeding) for the parties who engaged in the spoliation; in jurisdictions where relevant case law precedent has been established, proceedings possibly altered by spoliation may be interpreted under a spoliation inference, or by other corrective measures, depending on the jurisdiction."

So, if you typically do not go about wiping your hard drive with DBAN , and you suddenly wipe it clear of any traces of possibly existing evidence with 5 iterations the night prior to confiscation of your devices, that may seem a bit off and considered to be an obstruction of evidence. However, any harsh accusations could easily be plausibly denied if you could prove that you wiped your hard drive on, for example, the fifth of every month, just as a habit that you have gotten into; this claim has the potential to wipe that evidence straight out of a court room and maybe even acquit you.

With that said, it would be beneficial to make a routine of cleaning your devices, keep private logs of your cleaning schedule, and do not share them with anyone – more often is better, automating these processes would be ideal. After all, if the FBI knows that you do your cleaning on the fifth of every month, they may specifically wait until the fourth to raid you and seize your devices for further investigation.

Plausible deniability in the cyber realm goes hand-to-hand with encryption, so learn to use it in every aspect of your Internet usage, if safe to do so. Remember that the use of encryption will make you more suspect to intelligence agencies and other intrusive parties, so it is important that you normalize it to you're your traffic usual and consistent. Even though the heavy use of encryption technologies may appear abnormal to anyone

looking for unusual traffic, if you make a habit of it even for using encryption for everything, even chatting about things like your favourite type of pizza, then it shows that it is just a normal thing that you do during your day-to-day basis. Encrypt everything all the time, and you can simply explain that you are a cypherpunk without seeming like a criminal. It is one thing to use encryption for everything, but it is another to only use it for specific activities. Someone analyzing traffic logs will notice unusual use of encryption mark and correlate it to something bigger, thus marking you as suspect (an example of this is provided in the "Correlation Attacks" section of this reading).

You could also set-up a LUKS killswitch for your encrypted (FDE) HDD. Explained, it is "a patch for cryptsetup which adds the option to nuke all keyslots given a certain passphrase. Once the machine is rebooted and you are prompted for the LVM decryption passphrase. If you provide the nuke password, all password keyslots get deleted, rendering the encrypted LVM volume inaccessible." You can learn more about this subject here: https://www.kali.org/tutorials/emergency-selfdestruction-luks-kali/.

It will greatly benefit you to learn more about how to destroy evidence and avoiding getting caught doing when doing so, ensure that you are capable of using plausible deniability to your advantage.

Database Breaches & Conscious Account Registration: Understanding Breaches

Before we dive into creating our very own fabricated persona, we first need to understand where our data is being stored. In the *relations* section of this reading, we addressed that personally identifiable information (PII) is stored in databases all over the Internet. Remember, the Internet is nothing more than an interconnected network of autonomous systems, so these databases actively sit upon insecure systems and networks that are facing the open web. Hackers frequently compromise these systems; as a result, user tables containing sensitive personally identifiable information are stolen. These databases are traded and sold among the Internet's black market and cyber-crime rings, some services even offer free database sharing.

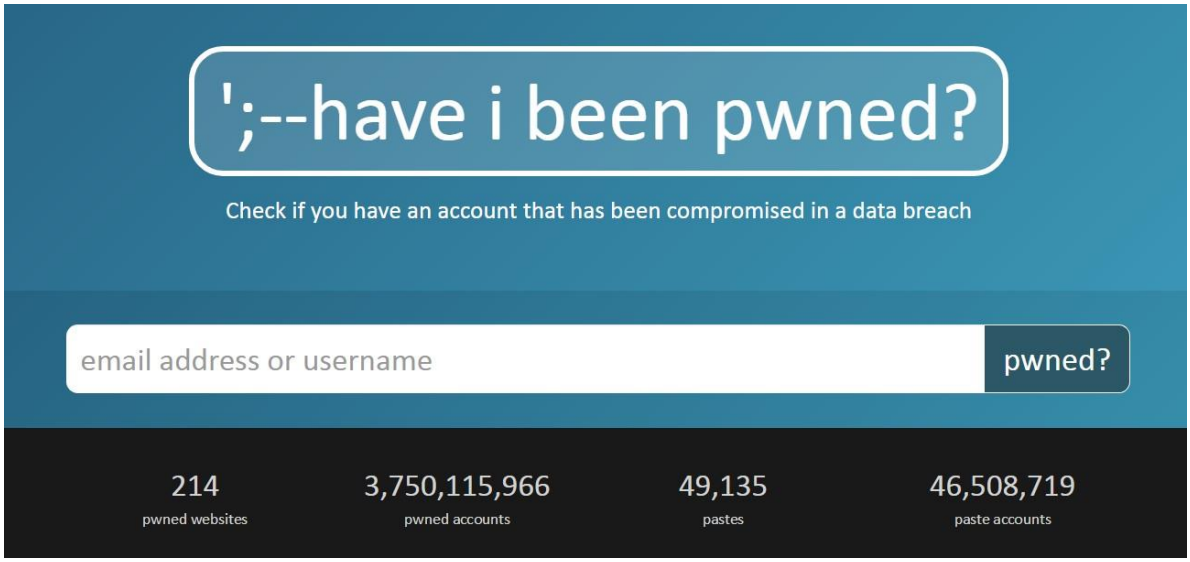
"These databases would cost you thousands in criminal networks, and we provide them for free." – http://databases.today/

We have reached a point in the age of the Internet where no data can be assumed to be genuinely secure, even if a website claims such. It is important that we take the necessary time out of our day to understand how and why all websites and services should be assumed to be insecure, and evaluate what defensive operational security measures can be put into place with the goal of preventing these malicious users from being able to do anything with the information that they obtain.

If you follow any news outlets, you have probably heard of some of the recent database breaches that resulted in the mass leaks of user information, some examples are: Ashley Madison (2015), Comcast (2015), Adobe (2013), Neopets (2013), Snapchat (2014), YouPorn (2014), Tumblr (2013), VK (2013), LinkedIn (2012), and the list just goes on. Even the National Security Agency had an archive of tools, vulnerabilities, and exploits stolen from them, which was shared publicly by the Shadow Brokers group. For more technical information regarding breached databases, I recommend the Vigilante.pw breached database directory.

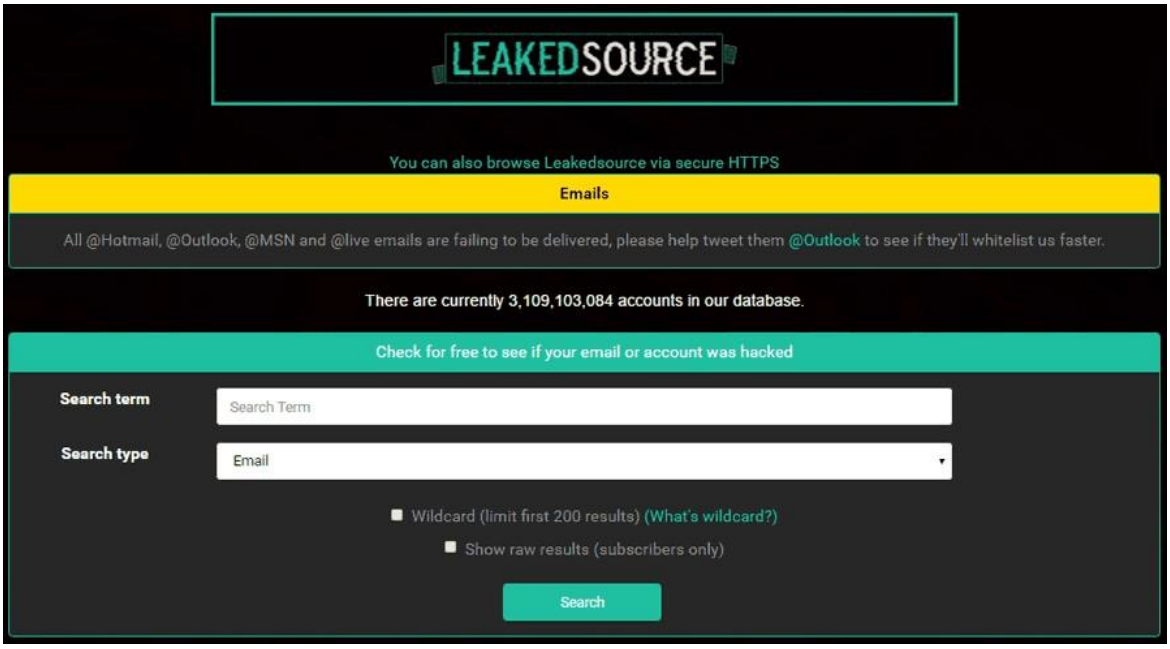
If the NSA is running into security issues, would you not think that all services and companies share the potential to be hacked? Everyone is vulnerable, no one is secure; in a sense security is an illusion. As Christopher McCandless said, people are "conditioned to a life of security, conformity, and conservation, all of which may appear to give one peace of mind," so do not be fooled by the illusion that we call security.

Security breaches are inevitable for anyone; databases are stolen every day, and even publicly leaked by services, such as Databases.Today. Hacked database sharing services frequently come-and-go, but just know that databases are always being leaked and traded somewhere on the Internet. Some as large as MySpace (359,420,698 account credentials stolen), and others as small as your favourite online forum, like FinalFantasyForum.com (3,528 account credentials stolen).

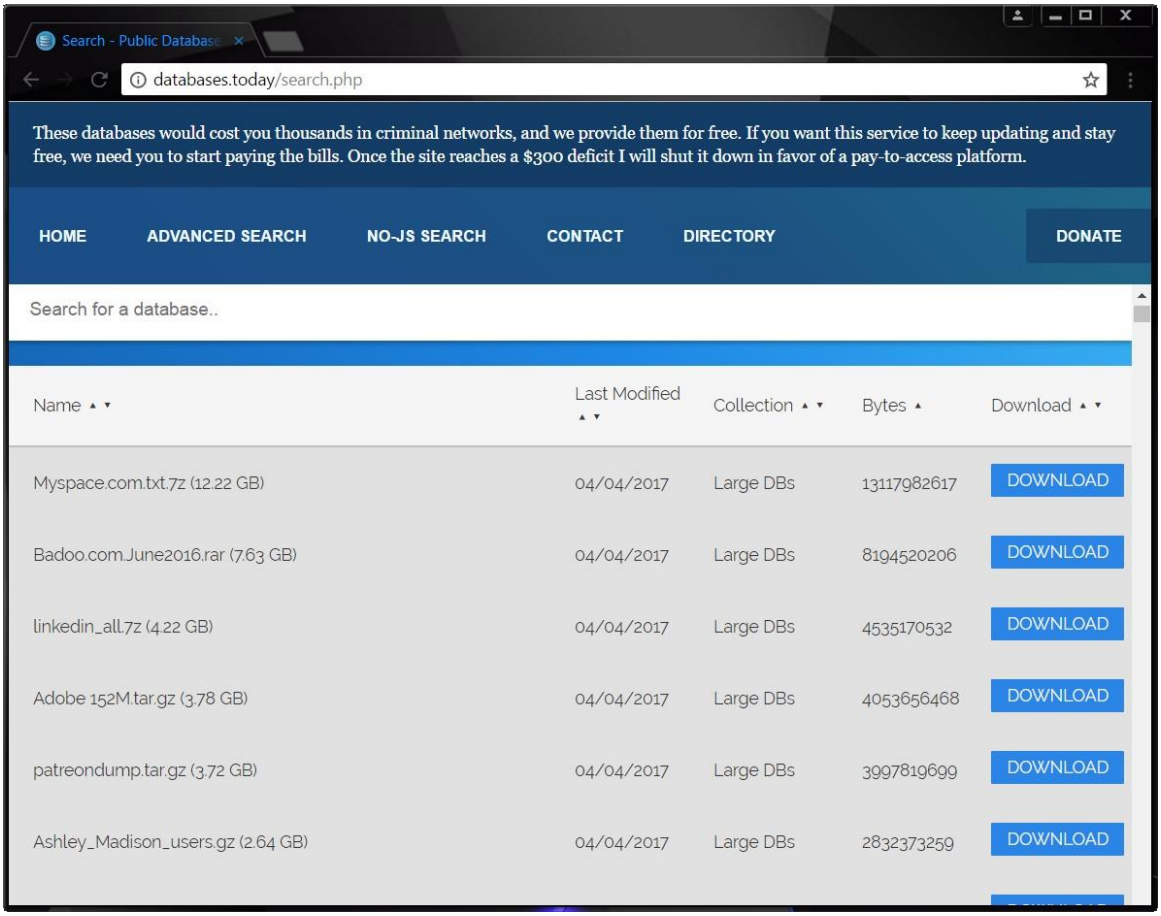


3,750,115,966 accounts among 214 database leaks on www.haveibeenpwned.com

3,242,292,368 accounts among 2,680 breaches on www.vigilante.pw



LeakedSource, a past popular hacked data search engine, raided and shut down.



A screenshot from the free search utility of a hacked database hosting service, http://databases.today/

Every day, databases that are filled with your account information are shared amongst the hacker underground. Every day, both deserving and innocent people are attacked as a result of malicious users having access to sensitive personally identifiable information. If you use the Internet like anyone else, then you have the potential to be vulnerable to these attacks as well. It is important to understand what you can do to prevent these security breaches from having a significant impact on your privacy or anonymity.

When a database is stolen, only the attacker will have access to the stolen data. After the initial breach and extraction of the user table from the database, the attacker may decide to do one of many things: sell, trade, share or choose to keep the data private, or even mine the data for personal reward.

There is a large market for buying, selling and trading databases. After a few months of a database being sold and traded, it becomes fairly saturated within cybercrime rings, and once the value has significantly dropped due to the data no longer being "private" or "fresh," eventually someone will likely leak that information to the public since it no longer holds value within these rings. An example of a popular database collector is Keen from Vigilante.pw; on Vigilante.pw a list of databases can be found, and you can see if they are tagged "private" or "public" for yourself, these are all databases that are actively sold and traded daily. Keen has left contact details and openly states "add me on Jabber at keen@xmpp.ru if you are interested in [discussing] databases."

> "In an era of mega-breaches, digital packrats are amassing, swapping, and sourcing leaked passwords and other personal information like any other collectible." (*The Data Hoarders*, Joseph Cox)

People collect databases, and when they have billions of account credentials available in their arsenal, this arsenal is easily the result of over 1,000 different breached servers. This data makes it easy to sift through the information to identify a target of interest. Search tools (ex. *grep*, *sift*) allow an attacker to enter a string that they want to search for, and then the search tools will sort through every single account entry in seemingly no time at all. Depending on your storage drive (HDD, SSD), billions of account credentials can be sorted through, line-by-line, in minutes, with speeds varying based on computational power. Minutes is all it takes for a malicious investigator to almost effortlessly identify a single account amongst a billion other accounts.

As you can see, your account information can really get around and accessed with ease. This information typically contains a user ID, username, email, IP address, and we can only hope that the password is at least hashed. Here is one real example of a hacked SQL database entry:

> VALUES('4','**BlackRabbit**','570d05338b21a5a00aa57546abbd1119','gGaD5TD
> O','qYFr1UyQbf3QXln7MDXReo3OQM68WqBLAqsXk1RbVuLlGGYPNr',**'puppetzo ne@safe-
> mail.net**','**26**','./uploads/avatars/avatar_4.jpg? dateline=1399930771','100|
> 100','upload','2','','0','','1399928410','1400466926','1400465460','1400465457' ,'','0','','','','','all','Github:
> **https://github.com/maybeblackrabbit**\r\nKeybase: **https://keybase.io/blackrabbit**\r****nJabber:
> **moonlight@jid.su'**,'1','1','0','0','1','0','1','0','linear','1','1','1','1','0','0','0','','','6','1','2','','','2','0','0','0','','1*
> *Inbox$%%$2**Sent Items$%%$3**Drafts$%%
> $4**Trash Can','','0','0','10',**'173.245.53.238'**,**'94.242.246.24**','-
> 1376438802','1592981016','**english**','20912','1','29','0','0','0','0','0','0','0','0','0'
> ,'1','2','');

This data sample is from a user who goes by “BlackRabbit,” I chose to use this data sample since this user had taken some necessary precautions to protect his personal information. Here we see IP addresses that he used, which is actually a Tor exit node. He also has his language set to ‘English’. We also see an email address that belongs to him, likely a one-time email address considering the address is called “puppetzone@safe-mail.net” We can also see that he has accounts on Github, Keybase, and the Jid.su Jabber server. We also have a hashed password, which could be a common password, but given the one-time email and Tor exit node, we will assume that this user likely used a one-time password.

BlackRabbit could have done a bit more to protect himself though. He could have used a one-time handle that is attached to no other accounts. Due to this database entry, even after the forum that he was signed up on ceased to exist, that “BlackRabbit” account is forever associated with the Github, Keybase, and Jabber accounts that he listed. BlackRabbit may be okay with his forum account linking to other accounts, but many people like to maintain their anonymity.

Just from this single data entry, we can create a simple profile of our target:

Alias: BlackRabbit
Language: English
Age: 26
Email: puppetzone@safe-mail.net
Github: https://github.com/maybeblackrabbit
Keybase: https://keybase.io/blackrabbit

Past IP addresses 173.245.53.238, 173.245.53.238

This is only some of the data that we pulled from the entry without investigating further. Databases carry a lot of information, and when investigated, they can reveal more than you may be comfortable with.

Database Breaches & Conscious Account Registration: Security Practices

Now that you are aware of what could possibly happen with your information after a security breach, we will look at what you can do to minimize the impact on your account security.

So, what can we do?

- Do not use the same username
- Do not use the same email
- Do not use the same password
- Mask your IP address
- Ask “how do I know if my information is in a hacked database and what do I do if my account data has been stolen?”

Do not use the same username

For the sake of protecting your own identity, use different usernames for every new account you create: never use the same username. Using the same username will make it easy for an attacker to link your information to other accounts, which could lead to the creation of your dox. Also, do not make your username too overly unique, like SikNESS_AXiOM, because that just makes it too easy to find any other accounts with the same username. Additionally, with a name like SikNESS_AXiOM, it pretty much guarantees that the user on any other website is you since who else would use a name like that? Go ahead, search the mentioned name on Google for an example of exactly what I am talking about.

If you do not want to end up like this person, then re-evaluate what you use as a username.

Instead of using the same username, or complex usernames, try to use shuffler aliases. A shuffler alias is an alias that is not unique, and unidentifiable to you. A shuffler alias should be nearly impossible to pick out and accurately identify you with in a crowd. An example of a shuffler alias would be “cat”, “russian”, “123”, or even “sky”. An alias with special characters, numbers, and words outside the English dictionary, are often very easy

to identify someone with, especially if you use the same name for every account you make (eg. SikNESS_AXiOM, again). By using a shuffler alias, you also cripple the attackers ability to search for your username in hacked databases due to an abundance of matches (how many times will the string “cat” appear in a pet forum database?) Seriously, do not use the same username everywhere unless you have a good reason to do so, and that reason aligns with the operation at hand.

Do not use the same email when registering accounts

Using the same email address for everything is a bad idea. If you were to use the same email for every account, your information will become very easy to piece together. If you are on 15 different forums, and 3 of those forums get hacked resulting in their databases being leaked, then someone could search for that one email, and sift through each database until they have a few matches with a simple *grep* search.

At this point, a person could easily have three descriptive database entries of yours that would also contain passwords of yours (hopefully they are hashed). If that password hash is cracked/decrypted then your account(s) could be broken into; I would hope that you do not use the same password for everything to prevent further unauthorized access. This is only one scenario where it is bad to use the same email. Do note that the ‘database search’ method that I just shared could also be used with something as easy as a username, if your username for everything is ‘jonnyboy381’ then I doubt there are any other jonnyboy381’s in the world besides you (use a shuffler alias!).

Do not use the same password

Not using the same password may seem obvious, but here are some general password rules to follow:

- Use special characters, numbers, lower AND uppercase letters, and consider making it a passphrase as well.
- Do not use the same password. Ever.
- Do not share your password. Ever.
- Treat your password with care; do not flaunt it around carelessly.
- Do not fall for phishing attempts, educate yourself about phishing.
- Do not make your password something that can be found in a dictionary (dictionary brute force)
- Ensure that your password contains no information that is identifiable to you (ex. names, birthday)
- Most services ask that your password be at least 8 characters long, but I would recommend at least 15 characters to keep it complex to prevent bruteforcing.
- Passphrases work splendidly as well, just make sure it is something creative and is not easy to guess. (ex. The 1 horse did not race today)

If you have a hard time keeping track of your passwords, you could either write them down on a notepad or use a trusted password manager. If you go with the first option, be sure to keep that notepad kept in a safe, secret place that only you know about. With passwords, there is no perfect solution, so do whatever best satisfies your threat model's standards.

Mask your IP address

IP addresses can reveal vital information, specifically your ISP and general geolocation. You can mask this by using proxies, Tor or a VPN. If you run into a competent social engineer who decides to target you, they may be able to gain access to your account information attached to your ISP by social engineering a representative from said ISP, using only your IP address to target you.

It is vital that you use a proxy of some sort as frequently as possible, especially when you are registering for an account since many databases register "registration IP" and "last IP used." This way, if you ever slip up when logging into an account, you only need to log out, turn a VPN on, and log back in to fix that mistake; this is only if you have a simple threat model, if you have a three-letter agency as your adversary, you may want to abandon any account that has ever been contaminated with your real IP information since it may later be used to identify you.

How do I know if my information is in a hacked database?

Visit a hacked database search engine, like https://haveibeenpwned.com/, and enter your username(s) and email address(es). This service (HIBP) will tell you if your account information has been breached based on the hacked data that they have available to them. You can also try LeakedSource which may have different data, among others.

Do not assume that your information has not been breached just yet, HaveIBeenPwned only has limited access to data, and there is much more information and databases floating around data-trading circles that may not even be reported on the media or by news outlets.

If you have experienced a breach of account security, change the appropriate passwords, disassociate yourself from any information contained in that account, and poison the data within the account of the hacked service. You will want to do whatever you can to disconnect your identity from that account, and plant necessary data poisoning practices where possible.

Building a Persona

Precursor: Use some type of protection whenever you create an account. *Remember, everything is logged, everything is tracked, everything is cached, and* ***your digital footprint is not going away.*** *Use a VPN, use a proxy, use Tor, encrypt your communications –* ***protect yourself.***

Everything is circumstantial, and so is your persona. Creating your new fabricated identity is entirely up to you, I cannot comfortably provide you a step-bystep guide on how to do so, but I can provide my personal advice. This is all this chapter is:personal advice, tips, and ideas. Take this all in with a grain of salt, but in my eyes, every persona is a circumstantial persona.

Nearly every persona that I have ever made was created with *purpose.* There was an end-goal with the persona in mind. Without purpose, I find that the persona is quickly abandoned. When creating a persona, identify *why* we are creating it; what is our end-goal with this persona, and what steps during the persona's creation can we take to meet this end-goal?

Our identity will consist of "seeds" of disinformation, we keep on nurturing these seeds until our fabricated identity blossoms into a truly convincing identity. We must treat our identity's information with care in order to meet operational goals; carelessness is a major violation to our goal of secrecy. Something as simple as persona contamination, or cross-contamination, can ruin the integrity of our identity, and the success of our operation.

Maintaining a fake identity can be a very daunting task, but it can pay off greatly in the end if this identity allows us to meet our operation's end-goal.

For some, they may just want to use an identity to avoid being doxed. It can be very satisfying when we login to an account one day to see that an adversary has tried to dox us, and they actually just doxed our fake identity instead. We used our "Let Them Find Us" concept to compliment our persona, they thought that they found our real identity, published our fake dox, and we are still relatively safe. The dox may hinder our operation, but at least it is less likely to put our real identity at risk.

So, how do we go about creating this brilliant fake identity of yours? Well, you are going to need three basic things: persistence, a brain, and common sense. Creating a persona can get extremely tedious, time-consuming, and boring after awhile. To be clear, there are a lot of different approaches to creating a persona. Do it however you please, I will just be going over some fun ideas that we can try.

Identity generators.

For instance, we can use a web service to get an idea of what our identity's profile should generally look like.

1. Visit https://www.fakenamegenerator.com and generate the base of a new identity
2. Below is an example provided by this service:

PERSONAL
Name: Jeff H. Garcia
Address: 4847 Carter Street, Belleville, IL 62221
Mother's maiden name: Guzman
SSN: 356-60-XXXX
Geo coordinates: 38.416021, -89.998579
Phone: 618-746-2978
Birthday: November 10, 1994
Age: 21 years old
Zodiac sign: Scorpio
Email Address: JeffHGarcia@jourrapide.com
Username: Satim1994
Password: aeNocho0ah
Website: debrafpawnshop.com
Browser user agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 **FINANCIAL**
Visa: 4716 0563 8225 5221
Expires: 1/2021
CVV2: 286
EMPLOYMENT
Company: Joshua Doore
Occupation: Process technician **PHYSICAL**
CHARACTERISTICS
Height: 5' 10" (178 centimeters)
Weight: 189.9 pounds (86.3 kilograms)
Blood type: O+

Now that we have some personally identifiable information to work with, we could save it in a text editor and adjust the identity to our liking. Remember that this is our identity, we can change whatever we want. For example, I would personally change the username, and I'd also go as far as to make another Gmail account or something with my persona's name in it to be that much more convincing.

XDD is another interesting project, a false identity search engine. They describe their service as "[an actual] list of [x] million people, indexed by the WRONG address, name, phone, and SSN. This data is fictitious. Any resemblance to an actual person, living or dead is purely coincidence […] The fake identities in this site are designed to rank higher in search engines compared to the other companies listings. In the case of phone numbers and social security numbers, our sites rank first. This fact will keep some of the curious away from attempting to pry into your true identity."

- Fake US Identities: http://xdd2.org/

- Fake UK Identities: http://www.xdduk.org/

Again, take all of this with a grain of salt. This is a starting ground, but an identity generator should not consist of an entire “identity.” A web service is never enough, nor should we rely on any single identity generating service… it is sloppy practice. I believe that handcrafting identities is the best approach.

Social media.

Once we have our email set-up, we may want to create some social media accounts. If we are creating social media, I assume that we want a public-facing identity. This could be useful for throwing off doxers and other Internet stalkers and potential harassers.

Additionally, it is beneficial to understand good privacy settings aid us in limiting what account information is publicly available. Be sure to carefully consider what options you have for privacy and security account settings for all social media accounts. This sounds straight-forward, but it can be easy to forget to set your privacy settings; always review your accounts privacy settings.

I will go through some very straight-forward security and privacy settings considerations for social media accounts. I will only cover Facebook, Twitter and
LinkedIn, but all social media is similar, so figure them out on your own if you need to.

Facebook.

We are trying to make it look like you actually have a social life right here. If we just make a Facebook, and change all of the privacy settings to "Friends Only", including our friendslist, then nobody will even know that it is a friendless dummy Facebook. If they ever go to dox us, they will find our dummy Facebook and likely use that as further support the validity of the dox.

- *Security and Login* settings: https://www.facebook.com/settings?tab=security
- *Privacy* settings: https://www.facebook.com/settings?tab=privacy
- **Tip:** To view what a stranger can view on our Facebook account, we can:
    - Visit our own timeline while signed in
    - Direct our eyes to the bottom right of our cover photo, look for the "..." panel beside "View Activity Log"
    - Select the "..." panel, select "View As" will show us what our Facebook looks like to somebody with no mutual friends.
- **Tip:** Use a fake last name, first name is optional. Let's be real, many of us need Facebook for real-life social networking. As long as our identities are compartmented well, this shouldn't matter too much, but we will discuss identity cross-contamination very shortly.
- **Tip:** Disable "account lookup by email/phone number" feature

Twitter.

- *Privacy and safety* settings: https://twitter.com/settings/safety
- **Tip:** Enable “private account” to hide tweets from non-followers
- **Tip:** Enable “Password reset verification” feature in the main settings page ◦ This will protect adversaries from viewing your partial email address ◦ Enabled “password reset” page:

◦ Disabled “password reset” page:

LinkedIn.

- *Account* settings: https://www.linkedin.com/psettings/account
- *Privacy* settings: https://www.linkedin.com/psettings/privacy
- *Communications* settings: https://www.linkedin.com/psettings/messages
- **Tip:** Set a custom URL to something other than your real full name. Also, consider just setting an initial for your real last name. Less information is better privacy, but that trade-off for privacy is ultimately up to you job seekers.

- **Tip:** Be careful about what you decide to share in job descriptions, this can be revealing of your company's internal infrastructure, and bad operational security practice professionally. Attacks performing OSINT will check the LinkedIn profiles of employees to understand the company better.

The photos.

Consider collecting an archive of pictures of one certain person to use with your alias. We could search Instagram or Facebook for a random, unpopular person; save all of their pictures, and use them as our own. This may seem unethical, but it is just an idea. There really is not any way to ethically use someone else's photos without revealing our real identity. Remember: don't steal identities, fabricate them.

Alternatively, we may want to develop an identity using our own photos. This is much easier to do if it allows us to safely meet our end-goal without dangerous information exposure, but this has obvious operational security flaws.

Be wary of metadata contained inside photos, this specific type of metadata is called Exif (Exchangeable image file format) data. Exif data can hold data such as technical information (unique ID of device) and the geolocation (GPS coordinates of where the photo was taken).

According to Wikipedia, in 2012, "John McAfee [founder of McAfee Anti-Virus) was arrested in Guatemala while fleeing from alleged persecution in Belize, which shares a border. Vice magazine had published an exclusive interview on their website with McAfee "on the run" that included a photo of McAfee with a Vice reporter taken with a phone that had geotagged the image.The photo's metadata included GPS coordinates locating McAfee in Guatemala, and he was captured two days later." (Exif, *Wikipedia)*

Most social media platforms and popular image hosting services strip Exif data upon being uploaded, but consider this to be a non-default luxury; you should strip an images EXIF data prior to sharing it. Alternatively, you can manipulate the Exif data to hold disinformation using a tool such as ExifTool. ExifTool can be used to read, write, and manipulate image, audio, video, and PDF metadata. There are also online services and other tools that you can use to strip Exif data, but local is better.

The wrap-up.

I feel that most people should be more than capable of finding creative ways to develop a fabricated persona and make it look legit while optimizing privacy settings and features. It is up to you to develop the identity however you like, but just remember to never, ever link that persona to anything outside of the persona's compartmentalized identity, like a personal email or exposing image (visual or meta).

Something as simple as linking a personal email to an operation can cripple everything, as proven by Alexander Cazes, the founder of AlphaBay, when sending password reset emails from his personal email for the darknet black market (Pimp_Alex_91@hotmail.com). This type of discussion is covered more when we discuss *persona contamination* and *compartmentalization*.

From here on out, you are on your own with creating your persona. Be creative with it, but be cautious and compartment your identities well, and keep an eye out for revealing metadata.

When it comes down to it, do what you have to do to satisfy the operation's end-goal. As we know, every identity is entirely circumstantial and unique to our operational goals.

Persona Contamination:

Avoiding Cross-Contamination of Identities

What is persona contamination?

Persona contamination occurs where there is a link between identities, whether they be real or fabricated; persona contamination is the cross-contamination of personas.

That contamination will occur when they lead to correlation, allowing an adversary to identify who is operating behind the mask. A high-level example occurs when personally identifiable information is leaked, causing an adversary to identify *Identity A* by using *Identity B*'s information. In short, persona contamination is all about dirty correlation.

It is always important to isolate identities through good identity compartmentalization practices. Our identities should not ever interact unless it is for the long-term benefit of the operation.

Keep in mind that you should not be sharing any of what you do on these identities with anyone who is not on a need-to-know basis, this includes your friends, family, or even your life partner. It is just a bad idea to have "loose lips", should the adversary (ie. feds) begin to interrogate your friends and family. CIA agents operate around OPSEC rules 24/7, so hackers should be just as secretive about their operations if they want to avoid operational conflict. So do your friends and family a favour by lying to them about your operational activities.

The Communist Party of South Africa said in their article *How to Master Secret Work ,* "Carelessness leads to arrests. Loose talk and strange behaviour attracts the attention of police and "izimpimpi" (I don't know what they meant by "izimpimpi", but let's go with it). Secret work needs vigilance and care. Rules of secrecy help to mask our actions and overcome difficulties created by the enemy."

Adding to this with a quote from another B3RN3D article, "Often, the vanity of your project will tempt you to share the details with someone else even though you know it is safer to keep them a secret. In hindsight, you'll come to realize that you've created a liability but for those few moments of discussion, you will irrationally determine it was worth it." (*Lie to Me, Please*, B3RN3D)

Despite our focus on the digital realm, real-life OPSEC is still vital to succeed in our operations. In real-life we practice communications OPSEC by speaking on a need-to-know basis. That said, your second-life as a hacker appears glamorous and magical to the rest of the world. Of course, others will find it interesting and ask us crazy questions, but nobody actually cares about what you are doing in your second life. If they do care, they become a threat; if they don't care, they still become a threat.

If you tell someone about your second life as a hacker at a local bar, I promise that later that night, you will quickly realize what a fool you made of yourself. At this point, you will realize you only made a new threat to worry about. The anxiety and stress will catch up to you, and it won't feel good.

With that being said, let's make a simple rule to avoid all of this stress and anxiety: *just stop talking.* Seriously, no one *actually cares* about your second identity, you are just another person (referring to the *Just a Man* philosophy).

Maintaining a persona and knowing when to let go

There comes a point in our fabricated identity's career where our real identity may be discovered, seeing as people are consistently doxed, and that trend is not going away anytime soon. For this reason, it is important to prepare for the postmortem damage that occurs after our alias' de-masking.

Assuming persona contamination has been avoided until this point, our adversary's investigators may have only correlated a single piece of information to our real identity. At this point, our adversary becomes a physical threat to us, depending on the circumstances, as it may be in our adversary's interest to have us jailed, assassinated, attacked, harassed, robbed, or something of the likes. We want to do our best to keep the threat away from being physically threatening to us, as it will greatly interrupt our operation. When an adversary becomes a physical threat to us, that goes out of the scope of this book, and may cause great troubles to our lives, especially if we become caught up in the American legal system (you don't even need to be American to be held hostage in their legal system, surprise!).

Ensure all information on each individual persona is as isolated as possible, preferably in different encrypted, compartmentalized spaces. If an adversary gains access to a system, it is critical that they cannot associate that system with other identities or discover more sensitive personally identifiable information. The better our digital hygiene is, the more we mitigate the possibility of a digital adversary becoming a physical threat.

Something else that you need to do is have layers, so simply having an initial cover identity is not sufficient. Once you have one cover identity, you then start creating sub-aliases from that. It can be better to have multiple cover identities so that when you get paranoid and you believe one has been compromised, you can phase it out rapidly and move another one into place.

By definition, a persona is an assumed identity or character or the mechanism that conceals a person's true thoughts and feelings, esp in his adaptation to the outside world. Though it may hurt to toss away the persona that you have invested so much time, effort, and hard-work into, remember that it still is just a persona created to cover yourself for when you mess up.

As said before, building up a persona for your secret hacker identity can be time-consuming and tedious, so you don't want to mess up. You can avoid messing up in that sense by never contaminating it. How do you do

that? For starters, let's look at "The 10 Hack Commandments". I want you to read over this list a few times over and think every single rule listed here through and why you think the rule is on this list.

Rule 1: Never reveal your operational details
Rule 2: Never reveal your plans
Rule 3: Never trust anyone
Rule 4: Never confuse recreation and hacking
Rule 5: Never operate from your own house
Rule 6: Be proactively paranoid, it doesn't work retroactively
Rule 7: Keep personal life and hacking separated
Rule 8: Keep your personal environment contraband free
Rule 9: Don't talk to the police
Rule 10: Don’t give anyone power over you

And above all, remember the magic four words: keep your mouth shut!

When you speak to your online hacker friends, be careful. Many may have ulterior motives. A general rule of thumb is to not make strong personal relationships on hacker forums and whatnot, considering you never truly know who you are talking to.

When your anonymous hacker friend is betrayed, they may attack you. When they get bored, they may betray you. Malicious-minded hackers are unpredictable and cannot be trusted. After all, look at LulzSec; how they were caught, how Sabu betrayed his comrades, and the feds closed in on all of them.

Anarchaos - Told Sabu how he was on probation at some point and received a drug charge. Information was easily used to trace him down. He was later arrested.

Palladium - Told Sabu whenever he changed aliases and other personal information. Information was also easily used to trace him down. He was later arrested.

Take note that Palladium contaminated his persona by sharing his new personas with Sabu so carelessly. It is seemingly pointless to switch identities and fallback to a new cover if you already admitted that you are someone who already has a profile being built up. Palladium just allowed "them" (doxer, gov, whoever) to continue profiling his alias as if nothing happened. This could have been prevented if Palladium had fully "shed" his old persona and started out with a brand new, fresh one -- Kind of how a snake sheds its skin; once it sheds, it never goes back or clings to it.

Several other members were caught in similar ways just because they contaminated their persona by telling Sabu things about themselves via instant message, thinking of him as a friend or co-operative.

When you are discussing anything with anyone online, consider these rules. Let's call these the "*Rules of Anti-Contamination*":

Do not include personal information in your nick and screen name.
Do not discuss personal information in the chat, where you are from...
Do not mention your gender, tattoos, piercings or physical capacities.
Do not mention your profession, hobbies or involvement in activist groups Do not use special characters on your keyboard unique to your language
Do not post information to the regular internet while you are anonymous in IRC.
Do not use Twitter and Facebook
Do not post links to Facebook images. The image name contains a personal ID.
Do not keep regular hours/habits (this can reveal your timezone, geolocation) Do not discuss your environment, e.g. weather, political activities,

Again, everything is circumstantial, and so are your operational rules. Adjust them as necessary to fit the needs of your operations' end goals.

Lather, rinse, repeat; stay clean; never contaminate.

Compartmentalization: Identity Management

Precursor: In July of 2017, I wrote an article about managing pseudonyms through compartmentalization for *AlienVault*. I am reusing that content here since there is no point in rewriting a legacy. (*Managing Pseudonyms with Compartmentalization: Identity Management of Personas*, CryptoCypher)

The Need for Identity Management

"Everything is circumstantial," this saying is especially applicable to the creation of every individual persona that we make. When there is something that we would like to achieve, we may create a persona specifically tailored to the requirements needed to accomplish said goal, as simple or complex as the goal may be. Fabricating identities is a popular tactic among the spycraft industry, and for good reason: it works.

While fabricated personas may seem straight-forward at a glance, a persona is actually quite time-consuming and tasking to both develop and maintain. It is critical that every individual persona is understood in great detail in order to obtain optimal results; otherwise, an entire operation can fall apart.

There are three key factors that will be looked at in regards to identity management:

1. OPSEC model
2. Identity compartmentalization
3. Mental health & psychological vulnerability

The First Factor: OPSEC Model

Previously discussed within the *Threat Modeling* section of this reading. The OPSEC
Model is the set of rules that are followed for a particular operation. Refer to the *Threat Modeling* section for more information regarding OPSEC models or just read this blog.

The Second Factor: Identity Compartmentalization

What is compartmentalization?

To compartmentalize is to divide something into sections or categories. Identity compartmentalization is the process of managing identity segregation to mitigate the risk of leaking information to the wrong parties (ex. persona contamination). Put simply, keep your lives separate from one another, no different than a married couple having an affair.

How do we compartmentalize our identities?

Know your identity; know your fabricated identity just like you know your real identity, memorize whatever information that could possibly be needed, and then some more. You can never know your identity too well.

Avoid persona contamination; do not speak about your other identities to anyone outside the scope of your OPSEC model.

Apply data poisoning; logically make identity personalities separate, and give them different backgrounds to prevent cross-identity suspicion.

Be organized; document your identities, it will help you know your identity better by organizing facts in a structured manner. Store these identity documents on an encrypted partition, preferably hidden and outside the cloud so no one can find them. Assume your adversary will intrude on your base site to seize devices and documentation.

Additional reading on compartmentalization theories

B3RN3D also has some good blog posts for strategically compartmentalizing identities. Said blog posts include an exemplary OPSEC model, using psychology to manage state-dependent memory and an Event Boundary theory that may be worth checking out; although, not mandatory.

- Braintricks for OPSEC
- Event Boundaries: Helping to Compartmentalize Your Operations
- Defining Levels of OPSEC to Your Identities
- Perspectives of OPSEC Models

The Third Factor: Mental Health & Psychological Vulnerability

Managing multiple identities is very stressful and taking on the human brain since we must always be conscious of everything we say and do. When using a persona, we should always be mindful of contradicting our own words and views, cultural misunderstanding leading to unfitting communication, maintaining appropriate stylometry, among an infinite number of other possibilities. When operating behind a persona, we are not supposed to be ourselves, we must be mentally prepared to manage our identities without failure.

Lindsay Moran, an ex-CIA operative, expresses the stresses of managing multiple identities in her book *Blowing My Cover: My Life as a CIA Spy* (99 cents for a used copy on Amazon). She tells the story of the personal sacrifices she had to make in order to properly compartmentalize her identities to maintain operational security as a CIA agent. OPSEC and identity compartmentalization made it difficult to maintain a personal social life, just as the same things make it difficult for some hackers to have personal relationships.

During Lindsay's CIA training, she had to remain secretive about the entire year-long interview process. The CIA is built on secrecy just as many security circles are, so members and agents must be conditioned to continuously practice a lifestyle built around OPSEC. This is a very lonely journey since your work and operations can consume your entire life, so just like a CIA operative, persona contamination must be considered a sin, secrets must be kept from those close to you.

Let security logic guide you, not paranoia. When OPSEC becomes a daily practice, you will become better at lying on demand and mitigating attack vectors onthe-fly. You will become pro-actively aware of the car that has been behind you for 2 or 3 blocks in worry of being trailed, concerned about network monitoring in every possible atmosphere, and paranoid that people are asking personal questions to leverage a targeted social engineering attack.

Some people say that paranoia is a good trait to have when practicing OPSEC, but paranoia can psychologically destroy a person through mental burn-out. There is a point where you need to draw the line and prioritize your human sanity over paranoia-driven OPSEC. With that said, let security logic and protocol guide you, not unreasonable assertions.

Don't forget your real friends. Basing your entire lifestyle primarily around one privately compartmentalized persona is dangerous territory in terms of mental health. Focusing strictly on "operational" pseudonyms may lead to a lonely place where you will eventually feel the need to find a friend. This leads to the risk of developing untrusted contacts acting as a false proxy for friendship; your entire friendship will be built upon lies, and if you make that personal, that could be emotionally damaging.

Drug markets and malicious cyber-circles are not the places for making friends, that is why we have bars and social events in real life. Do not let business control your life, it is critical that you continue to satisfy your psychological and emotional desires.

The take-away

Identity compartmentalization must be practiced by intelligence agency operatives, military personnel, darknet users, professional penetration testers, state actors, and just about anybody who needs to create a specific identity to carry out an operation. When creating an identity, an OPSEC model should be considered, and persona contamination must be avoided. We must know our identities inside-and-out, front-and-back, but mental health should always be a personal priority, regardless of the operation. Without good mental health, we are more prone to make mistakes due to personalized psychological vulnerability.

Real Identity Safety Considerations

Let's take some extra precautions that tie deeper into our personal lives.

I believe that if you are going through this much effort to create a secured persona, then you may have something to hide or you may just be very on-guard when it comes to digital privacy and security. To help put you more at ease, we will attempt to erase some of your current identity; the goal here is to make the real you a virtual ghost while maintaining your other compartmentalized identities.

The main subjects that will be addressed will be along the lines of social media, search engines, accounts, passwords, finding save alternative solutions to anything, and even safely answering unknown phone calls. So, let's go over a few things.

Social media – Social media is very telling; your personal information is plastered all over a series of webpages, some more public than others. People share a lot of personal information on social media, whether that information is a simple mention of a cellphone number, a professional email on LinkedIn, or a Tweeted picture with your friends and family at a local restaurant on Twitter. Any of these pieces of information can be very telling of our real identity.

If you are choosing to use social media, regardless of the privacy issues, then that is understandable. At the very least, consider this checklist for your social media:

- Are all of my posts and information set to "Friends Only"?
- Is anything on my social media account set to a "Publicly Viewable" setting? Not even your friend list, family relationships or an old profile picture?
- Have I searched every possible setting and made my profile as private as possible?
- Can strangers see anything personally identifiable to you besides your name?
- Does my publicly viewable profile picture or avatar include anything personally identifiable, such as your eyes, facial structure, or your property?
- Am I aware that my Facebook cover photo is always public, and if friends comment on or like it then potential attackers may look through their Facebook accounts in order to get an approximate idea of who I am, who my friends are, see if they have any pictures of me, my general location, potential workplace and potential schools?
- Am I aware that if any information is found, such as where I work or what school I attend, attackers may attempt to social engineer your employer, school representative or something along those lines, into giving up your personal information?
- Can I do anything to eliminate the possibility of the past two threats, if so, how?

- Am I using real information on social media?

- Your real friends already know who you are, where you work, and where you live, so could I publish some disinformation such as a false last name, hometown, spoken language or work information?
- Am I using a username that cannot be linked to other online accounts?
- Am I using a complex password that is not used anywhere else?
- Is an email address that is linked to any other account attached the social media account? If so, make a new email address and dedicate it to your social media accounts.

Search engines – Google is a great search engine, but according to several sources, specifically TechWorm, "Google has one big flaw. It traces your browsing history and has been in limelight for it user data scraping methods. It saves your search history, scans your Gmail, tracks your location, keeps everything you say from "OK Google," and a lot more. If you are using Google, then Google probably knows a lot better about your digital habits than yourself."

TechWorm continues explaining that, “Google tracks user data so that it can serve ads that are targeted just for you. Google says, it also saves data to give you better search results which may be quite true. Though Google allows users to opt out of Google’s interest-based ads and lets you delete your search history, it still saves enough user data to create a digital profile.” (*Worried about privacy, forget Google and try these search engines*, TechWorm)

The fact of the matter is Google logs and stores your search terms indefinitely. (*Why Google keeps your data forever, tracks you with ads*, ArsTechnica) However, Google does claim that they eventually make an effort to “anonymize” the data. Once 18 months have gone by, they further their efforts by “anonymizing” the unique cookie data that gets stored in logs.

So, what are some alternative search engines that you can use, do not log your activity, and respect your privacy? There are actually a couple that I would recommend, but I will only mention three of them: DuckDuckGo , Startpage , and the new default search engine of Tor, the new kid on the block: Disconnect . Make an informed decision to select a privacy-respecting search engine.

Phones – Do not answer the phone with your name, and do not use a personalized answering machine or voicemail message. Typically I would not write about something like this, but I have a huge pet-peeve, which we will get to momentarily.

A personalized voicemail message makes sense if you are using a business phone that is meant to be publicly known; however, it is simply not needed for a personal phone. You do not need to identify yourself, let alone your entire family tree in your voicemail. This immediately allows an adversary to identify you, and sometimes your family. Often times a low-ranking adversary will have trouble identifying the validity of a phone number until they can either check the voicemail for a name or have you verbally verify your identity over a phone call.

Sometimes attackers, scammers and malicious people in general will even go as far as spoofing their phone number to trick you into believing that the call is coming from someone else instead. An example of this would be if somebody was trying to form a dox; a document containing all of your personal information, they may want to verify a phone number, so they call you with their phone number spoofed to look like your bestfriend's landline; the number on your Caller ID may not be the real caller. With that being said, always answer your phone with the possibility of there being a malicious adversary on the other end of the call.

Obituaries – Consider taking some time to see if your name exists in any obituaries online. This may seem harsh, but it is in your interest to opt-out of obituaries considering that they list your family tree.

Real World Discussion – You can have astonishing operational security tactics, online anonymity, strong privacy practices, and an unquestionable persona, but this all can be rendered pointless the very moment you tell your friends, family or essentially anyone about what you do and who you are online. Keep your lives completely separate from one another through good compartmentalization. Never contaminate your persona. *Do not discuss your Internet activity with anyone, ever.*

Real Life Registration – People often sign up and subscribe for things without realizing where they are placing their information. Here are a few scenarios:

1. You are at Hot Topic, and you are thinking of purchasing some clothing and a few trinkets. You get to the counter with your desired items, and the cashier nicely asks you if you would be interested in registering to be a Hot Topic Club Member to get 30% off all sales, this membership requires you to subscribe to official Hot Topic emails, and for your information to be added to an account in a database identifiable to you specifically.

2. You are signing up for a gym membership, an account must be created in their gym membership database for you. They would like to have a picture of you just to have on file. So, you agree to their unnecessary conditions and allow them to keep a picture of you on file for the rest of your life even though it was not actually mandatory to do so.

3. You attend the Black Hat USA conference, and register using your real email address. Upon arrival, you are handed a badge with your personal information tied to it. As you walk around the conference, vendors scan your badge, harvesting your account information, and they later spam you with emails. Perhaps they even sell your data to unknown third parties.

There are a lot of ways that you can go about subscribing to mail lists and registering accounts in databases that we didn't even realize existed. Just because you are not yet receiving mail or email from somebody does not necessarily mean that you are not on a mail list, or just because you aren't receiving phone calls in regards to your gym membership doesn't mean that the gym doesn't still have that information about you on file.

You may be wondering why these even matters, but let me tell you this: there are some bad people on the Internet: malicious hackers, identity thieves, doxers, social engineers, and other parties who abuse their powers, and so forth. If one of these people, or even a private investigator, has their heart set on tracking you down, they may start calling stores and establishments such as your local Hot Topic and local gyms, attempting to trick them into giving up your information. This information could be anything from an email, phone number, home address to even your social security number. Frank Ahearn, a tenured skip tracer, discusses this multiple times throughout his book which will be linked in a moment.

The best way to defend yourself from attacks focused on social engineering third-parties is to remove that information in the first place. For services and appliances, call your provider and inquire about what you can do to add additional security to your account.

Transactions – Credit cards, debit cards and even gift cards leave trails. These trails are tracked by law enforcement, skip tracers, and private investigators. To prevent this, pay with cash or use cryptocurrency. Although, if you are using cryptocurrency, ensure that you take the appropriate steps to understand how you can mitigate blockchain/transactional analysis; otherwise, you’re going to slip-up. You should also know what types of transactions trigger red flags at your bank.

For more about erasing your real life identity, I recommend reading *How to Disappear: Erase Your Digital Footprint, Leave False Trails, and Vanish without a Trace* by Frank Ahearn. Frank is a tenured skip-tracer who shares how to erase your footprint, mostly offline, throughout his stories.

Part Five: Considering Operational Security and Counter-Surveillance

Locational Security

Internet users have to connect to the Internet from somewhere, right? People in the hacking scene typically talk about operating from one of two places:

1. Home
2. A public location (ie. store, mall, restaurant – anywhere with open WiFi)

Without going overboard, I believe that it is typically okay to work from home. You will want to consider using Tor and a trustworthy VPN together, as securely as possible. This isn't the perfect set-up alone, but it's a start. As long as you are masking your IP address in a sensible manner for your OPSEC model.

But what about if you decide to take your operations one step further, and use a foreign open network? Here are a few things to consider:

- Ensure that the open network is legitimate, a hacker may have set-up a fake WiFi hotspot
- Scout cameras out prior to operation, if possible
- Spoof your MAC address (?)
- Use both a VPN and Tor; at least one or the other, preferably both
- Dress in plain clothing
- Wear a hat or hood to hide your face
- Do not look directly at cameras
- Sit in a place where there are minimal screen reflections
- Sit in a place where bystanders cannot shoulder-surf to see what you are doing
- Try not standing out in a crowd
- Leave when you are done, again, without looking at the cameras

Take any security precautions that you may deem necessary. This is a very basic checklist that is designed just to give you an idea of what to consider. I recommend that you do your own research to see what information is visible to a network upon a device connecting to it and find out how you can hide or spoof said information. If you have any questions, look it up on a search engine like Startpage. No matter where you are, be sure to guarantee your own safety since no one else will.

Correlation Attacks

> "As the most important takeaway is that there is no privacy tool which will let you turn it on and turn off your brain. You always need to be thinking about what you are hiding, from whom, and how much effort they are likely to expend in finding you." (*Why TOR Failed to Hide the Bomb Hoaxer at Harvard*, The Privacy Blog)

The theory behind a correlation attack is simple: you are correlating two or more events to determine a conclusion. As simple as it may be, it is still highly effective and worth your time to avoid falling vulnerable to. You can use all the encryption in the world, but if an administrator can determine who you are based on obvious activity logs, then you have screwed yourself over from the beginning.

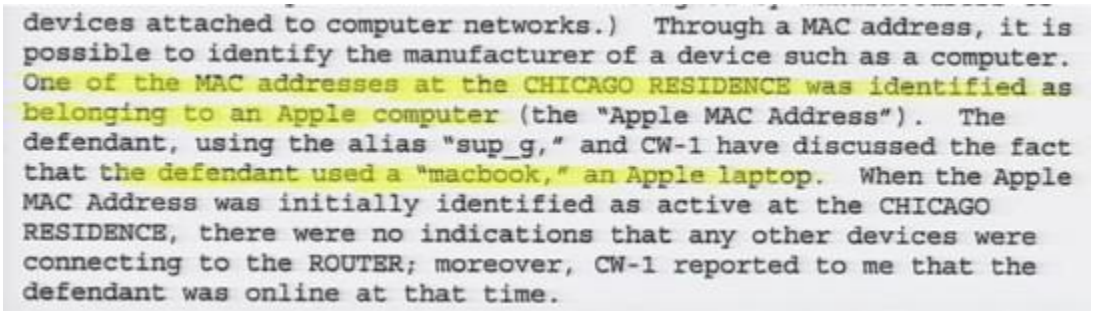
Correlation attacks are a huge OPSEC killer; these attacks can carry a heavy blow against your OPSEC if you fall vulnerable to them.

On December 16, 2013, a Harvard student attempted to delay exams by emailing a bomb threat to Harvard University stating that there are bombs hidden in two of four major buildings. The Tor network had been accessed from the campus WiFi in order to send the email. (*Harvard Student Arrested For Bomb Threat Tried And Failed To Hide Identity With Anonymous Browser*, Pamela Engel)

In order to find who sent the email, law enforcement did not have to attack the Tor network itself, but rather execute a correlation attack, an old-fashioned investigative method. By checking Harvard's network activity logs, they only had to look at who accessed the Tor network leading up to the hour of the email being sent to Harvard. The I.T. department only had to do a simple correlation attack to determine who was suspect, and getting Eldo Kim to confess was a piece of cake from there.

This method does not strictly apply to networks and activity logs. Correlation attacks apply to almost anything; it could be something as simple as mapping the timestamps on a target of interest's tweets from the last few months to determine what time zone they are living in. If you know a target's time zone, then you can also assume their approximate location; a few tweets have the potential to tell you approximately where someone lives, and what their sleep schedule is like.

In another case outlined in a talk by The Grugq, law enforcement was able to further confirm their suspicion of a cyber-criminal since they shared that they used a "macbook". Law enforcement confirmed that there was an Apple MAC Address coming from the suspect's room, and used that to strengthen their case. (*OPSEC:*
Because Jail is for wuftpd, The Grugq)



devices attached to computer networks.) Through a MAC address, it is possible to identify the manufacturer of a device such as a computer. One of the MAC addresses at the CHICAGO RESIDENCE was identified as belonging to an Apple computer (the "Apple MAC Address"). The defendant, using the alias "sup_g," and CW-1 have discussed the fact that the defendant used a "macbook," an Apple laptop. When the Apple MAC Address was initially identified as active at the CHICAGO RESIDENCE, there were no indications that any other devices were connecting to the ROUTER; moreover, CW-1 reported to me that the defendant was online at that time.

Excerpt from legal document

Whenever carrying out an operation or handling communications, always consider the possibility of a correlation attack, and re-evaluate the situation to compliment your end goal – even if that includes data poisoning. Understand the tools and platforms that you are using to carry out your operations; ask yourself questions like “what information does this store?”, and “how can I prevent information leakage?”

Stealthy Communications

Precursor: *Always register and access any account using some type of protection, consider a VPN and/or Tor; always have at least one layer of security when working with any online account. Many websites have two fields for IP addresses: one for the registered IP address, and one for the most recently used.*

The Internet is in its core essence is a series of interconnected autonomous systems that actively work together to maintain communications. In order for the systems to stay connected, information is actively shared between all systems involved; this is done through routing updates, information tables, and specific selection of protocols for the systems to communicate with throughout network stacks. Encryption will aid in the protection of the data you send and receive while it rides along these connections, routing the data through who-knows-what systems all over the world.

Since people and certain three-letter agencies like to eavesdrop on our communications to see what our latest favoured cat videos are, we want to spoil their ability to do so effectively.

There are a few things that we can do to secure our communications.

Email:

Do not host your own mail server, this isn't the 90's anymore. For sensitive messages, use PGP to encrypt your message contents. For your email services, find a privacyrespecting provider.

Clearnet email providers, with privacy interests:

- ProtonMai l
- RiseUp
- And more

Darknet email providers, with privacy interests:

- SIGAINT
- VFEmail

You may also want to consider using temporary, disposable email addresses, especially for websites with only a one-time use – I call this burn mail. I have been known to use 10 Minute Mail. You can find more by searching for something along the lines of “temporary email address”.

PGP Encryption:

According to TechTarget's article , “Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.

Pretty Good Privacy uses a variation of the public key system. In this system, each user has an encryption key that is publicly known and a private key that is known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

PGP comes in two public key versions -- Rivest-Shamir-Adleman (RSA) and Diffie-Hellman . The RSA version, for which PGP must pay a license fee to RSA, uses the IDEA algorithm to generate a short key for the entire message and RSA to encrypt the short key. The Diffie-Hellman version uses the CAST algorithm for the short key to encrypt the message and the Diffie-Hellman algorithm to encrypt the short key.

When sending digital signatures, PGP uses an efficient algorithm that generates a hash (a mathematical summary) from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version uses the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version uses the SHA1 algorithm to generate the hash code."

Understand what information you are tying to your PGP keys. An email address and other information may be tied to your keys. An example of this is when a darknet drug vendor got busted for registering the keypairs with the email "Adashc31@g .com". "Social media searches including the phrases "Adashc31" and "Adashc," led to Twitter, Instagram, and Facebook accounts linked to "Ahmed Farooq." Farooq's Facebook account made it clear that he was located in Brooklyn, New York." (*Timeline: Arrests of AlphaBay Vendors AREA51 and DARKAPOLLO*, DeepDotWeb)

An easy guide for using PGP encryption can be found here , courtesy of DeepDotWeb. Although, B3RN3D proposes that we let PGP die due to weaknesses in the keys and leaked metadata. Either way, PGP is still heavily used online and is worth being familiar with to secure your message contents when necessary.

Instant Messaging:

Instant messaging is just like email messaging, just a lot more instant as the name implies. Although, sending PGP encrypted messages back and forth can be a bit tedious, especially when you are instant messaging. It doesn't help that popular instant messengers like MSN, Skype, and Facebook Messenger monitors all of your account activity, including IP addresses, personal information, and worst of all, your plaintext messages. A nice alternative to these services that you can use is called XMPP.

According to the XMPP.org blog, "the Extensible Messaging and Presence Protocol (XMPP) is an open XML technology for real-time communication, which powers a wide range of applications including instant

messaging, presence, media negotiation, whiteboarding, collaboration, lightweight middleware, content syndication, and generalized XML routing." In more simplistic terms, XMPP can be used for instant messaging. XMPP is largely popular due to the easy-to-use Off-theRecord (OTR) encryption. XMPP is also known as Jabber. To use XMPP, you will need a chat client that supports it.

I would recommend that you use Pidgin for Windows, Gajim for Linux, and for Mac, you'll have to find a good client on your own. You can learn a little bit more about the clients, and what clients are available here .

You can really pretty much use whatever XMPP server you please. I am personally a big supporter of XMPP.is, and I trust that they do not log and try their best to respect their privacy. The administrators are the same as the ones who run CryptoWorld. I have several reasons as to why I trust them, but I won't bore them unless someone requests further details regarding their server specifically.

But the key thing in picking a server to use is that you need to feel that you can trust them. Look around to see what others in the hacking community use, ask them why they use that server, and what they recommend. Everyone has their preference, just like I prefer to use XMPP.is or RiseUp.net.

It is worth noting that regardless of what server you use for your account(s), it will not matter if they are logging you or you do not trust them for as long as you are always using OTR encryption.

They will only be able to log encrypted *jibber-jabber* (hah), that likely nobody will be even attempting. You can research anything further on your own.

It is common for users to have multiple XMPP accounts to separate identities. I have personally probably went through at least 20 accounts in the time that I have used it. I guess it is good for OPSEC to separate your identities to limit what knowledge specific individuals, or anyone, has of you. Most clients such as Pidgin and Gajim support multiple accounts to be used simultaneously.

You can find a list of different XMPP servers here. For specific information about other messenger solutions, like *Signal* and *Wire*, refer to this *Secure Messaging Apps Comparison* website.

OTR Encryption:

According to cypherpunks.ca, “Off-the-Record encryption, abbreviated as OTR, is a form of encrypted messaging which allows you to have private conversations over instant messaging by providing:

- *Encryption:* No one else can read your instant messages.
- *Authentication:* You are assured the correspondent is who you think it is.
- *Deniability:* The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured of message authenticity.

- *Perfect forward secrecy:* If you lose control of your private keys, no previous conversation is compromised.

It really is not that hard to set-up OTR encryption with any popular XMPP client. If you want to learn how to set OTR up alongside one of these clients once you have one downloaded, just do the following:

- Visit your preferred search engine
- Search "How to install OTR plugin on [preferred client]"
- Read
- Learn
- Do

Internet Forums:

Online message boards are a fantastic way to maintain a community feeling, share knowledge, and seek help for your problems. You can sign up, post threads and messages freely, and have a great time overall. Although, they are also the downfall of many people's personal security, since it is a source of *public relations*, something that we have already discussed.

A big issue with Internet forums is that people get too comfortable within their own community. They often forget that they are in public's sight, including potential hacker's and government agencies such as the NSA, CSIS or the GCHQ; all of which, participate in global surveillance .

Whenever you post on these forums, you will want to take some general security precautions. Usernames should never be unique or the same, different email addresses should be used whenever possible, passwords should always be complex and different, and you should always make sure that you do not post anything that could be considered *persona contamination*. If you insist on posting something personal, *data poison* it; do not post real information about yourself under any circumstances, ever.

And if at all possible, try to keep away from prying eyes by adjusting your forum account settings, since government agencies and potential attackers might try to do something like record every time that you appear online on the forum, which can be prevented by doing something as simple as selecting an option in your forum account settings that says *"Do not show when I'm online".*

Stealthy Communications, privacy and security resources

David from *The Many Hats Club* compiled a centralized list of privacy respecting resources. This is not a complete list, but it is a step in the right direction. If you need a solution for a specific need, then do your own research accordingly.

Indexed resources:

VPNs: Virtual Private Network providers (ie. CryptoStorm, Mullvad)
XMPPs: Instant messaging protocol, custom servers and OTR encryption
Emails: Privacy respecting email providers (ie. Protonmail)
Messengers: Pro-privacy messenger solutions (ie. Signal, Wire, Pidgin)
Encryption: Encryption solutions (ie. Disk encryption solutions, GPG4WIN) *Secure Deletion (Locally):* Securely wipe drives and files, system killswitch, etc. *Malware Related:* AV file scanner, malware search engine, etc. (ie. VirusTotal)
OS': Privacy & anonymity focused operating systems (ie. TAILS, Qubes-Whonix)
Hardware Wallets: Some local BTC wallet solutions
Forums: Anonymity & privacy discussion and resource sharing (ie. GreySec.net)
Websites: DNS tracking, WHOIS data, domain registration
Addons: Firefox and Chrome web browser addons
Browsers: Browser recommendations (Firefox, Tor Browser, Brave)
Email Forwarders: Email forwarding to protect email from harvesters
Email .onions: .onion emails
Email Anonymously: Send emails anonymously (use VPN/Tor to access)
Throwaway Emails: Temporary disposable email addresses, good for spam sites
Pastebins: Privacy respecting & encrypted pastebins for text dumps (ie. 0bin)
Email Lookups: Some hacked data search engines (ie. HIBP, LeakedSource)
Guides: Random guides
Pomf File Hosts: Pomf file hosting

Good strategy advice is timeless, but technology is developed on a finite timeline. Technologies will age-out and lose credibility as technological advancements are made. After this publication is released, I have no way of knowing what changes or revelations will be made. I will leave it in your capable hands to find modern solutions for achieving everyday security, respective to your OPSEC model.

If you have any questions, I would recommend the GreySec hacking forums, specifically the *Anonymity and Privacy* forum. This community is very helpful and will give you the hacker perspective on things that you are looking for. I am personally a staff member on GreySec and will more than likely engage in your thread if you present yourself reasonably. Do your research before posting; the GreySec community strongly believes in quality over quantity in terms of posting standards.

Leave No Trace

Every detective will need a lead for their case, and they only have that lead if you leave it behind for them to find. When you are carrying out operations, it is important that you minimize the trail of identifying data. In order to protect yourself from being identified, whether it be by removing the activity logs from a server or just by not making a Tweet every day. This is a pretty simple concept, but realistically there will be situations where leaving no trace is not possible.

When browsing the Internet, you can reduce the footprint that you have left by changing your user agent, forcing HTTPS for confidentiality, prevent tracking with a browser add-on like Privacy Badger or Disconnect. Consider using a VPN and Tor where possible to hide traffic usage, but remember that your ISP may find Tor activity suspicious, so configure these services respective to your own threat model.

Whenever you view a website, you do not want to leave any footprint behind, this means making sure that you change your user agent, use a proxy to cover up your IP address from the public eye, and use different passwords, emails, and usernames. If you are using the Tor browser, there will be a sliding-bar that allows you to configure your “level of security”, max it out. Disable Flash. For the most part, protecting your web browser is as simple as that.

When sharing pictures, you will want to scrub them of any metadata first, a type of metadata called EXIF data exists within pictures, remove this by using a tool like exiftool. EXIF metadata includes a large amount of random data, most specifically it can include geolocational, camera model, and filename (duh).

When communicating with others, I would recommend against storing chat logs as they could be used against you if the logs are accessed by an unauthorized thirdparty user. Depending on your operation, it may be beneficial to keep some logs for the sake of your own security and being able to defend your reputation.

Do not tell anyone anything that you would not be okay with having publicly viewable on the Internet. Again, MalwareTech is a good example of this (no shame), he shared personal information with some friends, which eventually leaked out to unwelcome reporters who essentially doxed him. If you won't say it on your personal Facebook, then don't say it anywhere. You don't ever know if the person on the other end of the wire is logging your conversation or not, or even planning to dox you in the long run. If they have data about you, and chat logs with your messages in them, and have their computer seized & searched, then the police still have whatever you said even though it was out of your control.

There will always be a trail somewhere, but the idea is to minimize it as much as we can respective to the circumstances; again, everything is circumstantial, logs are too.

Limiting Information Exposure

It would be fantastic if we could be content with leaving no traces ever, but that is not always the case. Due to this, we will want to be able to *limit information exposure* to ensure that we have full control of our information

and where it is being accessed. To limit information exposure means to control who and what can see which specific information, and when and where they see it too.

Right now, as of this very moment, silence is potentially a vital key to both your modern day and future operational security if you are operating under a particular persona. The information that an individual may leave around helps develop a footprint of data for that persona, it develops a paper trail in a sense. This is what is often referred to as a cyber footprint.

A cyber footprint should be seen as a vulnerability waiting to be exploited to cause harm to your real life directly, as it could act as evidence building up to your real arrest and imprisonment; not only that but your cyber footprint can be quite revealing as well which may dampen future opportunity. People will use your cyber footprint to locate you.

During a hostile reconnaissance operation that is being carried out against you, both law enforcement and malicious users online can gather a lot of knowledge surrounding your persona. The information gathered can, and will, be used against you. Whether this information is maliciously used against you in a dox, or in the court of law, it is all a threat to you. Your cyber footprint is proof of your existence, it is evidence. Without evidence, you are often acquitted of any charges, and without a cyber footprint, there is nothing to dox.

It would be easy to simply just say to never post or share anything with anyone online or offline; do not leave any solid evidence of your online existence; do not use any social media; do not use email or instant messaging services; however, none of these things are realistic. If you can manage to maintain a livable lifestyle by doing so, I am impressed. But if you are anything like me, you are going to want to make it appear as if you have been keeping your nose clean.

In short, you can practice the very basic operational security required for everyday communications by not sharing any personally identifiable information in public view, consistently using a VPN as much as possible, avoiding the use of the same emails, usernames, avatars, and passwords, and avoiding persona contamination. It really isn't that hard. Just don't go posting this and that everywhere and making yourself popular for whatever reason. It really isn't hard, don't try to act like anything special.

Everything has a trail. So, try your best to keep anybody in the future from finding the trail of your past. Nobody needs to know that information – your cyber footprint – besides you. Limit the exposure your information can experience, only you can do that right now, as of this very moment.

Destroying Your Persona

Everything is circumstantial; no how-to guide is written with respect to your operation's specific circumstances. You will have to develop and master your ability to maintain personas securely while simultaneously practicing OPSEC; in addition to maintaining a persona, you will also need to be able to identify when it is time to destroy a persona, or whether you should or not in the first place.

I am going to stress it yet again; *everything is circumstantial*. I cannot tell you how to best dispose of your identity. In some cases, you won't be able to delete data since what goes on the Internet often stays on the Internet. Although, if it isn't cached anywhere, deleting it may still help and potentially remove it entirely from public view.

To start, delete your accounts; JustDelete.Me is a directory of direct account deletion links to aid you in deleting your accounts from web services. If you cannot delete an account, then I recommend logging in with a masked connection and removing or altering all information possible. Online profiles, service and appliance accounts, documents, subscription lists, or whatever you have should be included in this process.

Put simply, avoid leaving loose ends by tightening things up where you can.

Cryptocurrency: The Cypherpunk's Currency of Choice

Digital transaction systems have become a necessity in today's society. Yes, we have Paypal, Stripe, and other solutions in place; however, these are not efficient enough, considering the lack of anonymity in these solutions. We need a decentralized system that allows for anonymous transactions, where we have the choice to reveal information on a case-by-case basis. We must have the ability to choose when and if we share information about ourselves to maintain privacy.

In *A Cypherpunk's Manifesto*, Eric Hughes makes the point that "privacy in an open society requires anonymous transaction systems", he continues, "until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy."

Later in this reading, Hughes makes the point that we must defend our own privacy if we expect to have privacy at all, exclaiming that we must take it upon ourselves to develop systems that allow for anonymous transactions to take place. Adding to this, Hughes states that "we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible."

Since the writing of *A Cypherpunk's Manifesto*, a new technology has arisen to serve as a solution for this problem: cryptocurrency; namely, Bitcoin. In 2009, Satoshi Nakamoto anonymously shared Bitcoin, the world's first decentralized cryptocurrency and worldwide payment system. This is a huge win for the cypherpunk movement. Since then, many new cryptocurrencies have been developed and become much more popular.

A cryptocurrency is a decentralized form of currency built on top of a complex system called Blockchain. Blockchain is a public ledger that holds a history of all transactions ever made. This is an important thing to understand since cryptocurrency is often assumed to provide a truly anonymous digital transaction system, but this is simply not true considering that all transactions ever made are published publicly. Due to this, many adversaries analyze Blockchain technologies to track and identify cryptocurrency owners, either for research purposes or to aid law enforcement efforts. There are ways to mitigate Blockchain analysis, which we will discuss in a moment.

Let's assume you would like to use Bitcoin. You will need a unique wallet. You can either use an online service such as https://blockchain.info/ to manage your wallet, or you can have a local wallet. If your wish is to maintain anonymity, I would recommend creating a wallet on a reliable, local system rather than storing it in the cloud. While a cloud-based wallet manager is much more convenient, you are providing your information to a third-party who may be subject to being hacked or subpoenaed. Consider your threat model for this decision.

As we discussed, there are a number of adversaries regularly performing Blockchain analysis. Some examples include the following:

- https://www.walletexplorer.com

- https://chainalysis.com
- https://scorechain.com
- https://blockseer.com
- https://coinalytics.co
- https://sabr.io
- https://elliptic.co
- http://numisight.com
- And many more

However, I want to draw attention to one research group in particular: The Bitfury Group.

In an article that I wrote for AlienVault, I explain that "The Bitfury Group released a whitepaper for their new Blockchain analysis algorithm with the goal of identifying the users behind digital transactions, dubbing their deanonymization solution as a "Bitcoin clustering" algorithm. Bitcoin address clustering is selfdescribed as "a process that exposes bitcoin users by determining which addresses belong to a single user through an analysis of Blockchain data. The act of clustering groups those addresses together, enabling investigators to link them to a single entity." (*The Bitfury Group Unveils Solution For Analyzing Related Bitcoin Addresses*, The Bitfury Group)

The Bitfury Group's analysis research should not be shocking to us. They perform Blockchain analysis, just as we should expect adversaries to do. The innovative part of this algorithm is that they are also analyzing publicly available information on the web, or as they call it "off-chain tag collection" to aid their clustering algorithm. There are two tag collection approaches that The Bitfury Group takes: passive and active.

Off-chain tag collection for clustering, passive tag collection:

The passive approach includes crawling the web for publicly available information, typically on public forums and user profiles. On the clearnet, they will analyze websites such as Bitcointalk.com, Twitter, and Reddit. On the darknet, they would analyze markets, forums, and services such as Silkroad, AlphaBay, and so forth. (*Automatic Bitcoin Address Clustering*, Bitfury)

Off-chain tag collection for clustering, active tag collection:

Bitfury describes the active approach as the "manual analysis of Bitcoin companies and data actualization procedures. The most common Bitcoin businesses companies are exchanges, marketplaces, mining pools and mixers. Some companies mostly use addresses with specific prefixes. As an address is a public key, for an unknown private key then to generate a specific address, one has to try many private keys, i.e., make some extra computational work. For example, Satoshi Bones casino uses 1change and 1bones prefixes and BTC-E exchange uses 1eEUR and 1eUSD prefixes. Addresses starting from 1MartinHafernikorn and 1Ninjaare also computationally demanding and can help to identify users." (*Automatic Bitcoin Address Clustering*, Bitfury)"

As we can imagine, cryptocurrencies are a huge step forward in achieving privacy-respecting digital transaction system; however, these systems are not perfect and contain some flaws. Due to this, we need to take the appropriate steps to mitigate analysis both on-chain and off-chain. We can mitigate on-chain analysis by using solutions such as *traditional send mixers*, also called a cryptocurrency tumbler, or a *shared coin joiner*, also called CoinJoin. We will focus on traditional send mixers.

Bitblender explains cryptocurrency mixing as "the process of obscuring where your coins came from, which in turn makes your digital trail much harder to follow." (Beginner's Guide to Bitcoin Mixing) Essentially, you have this system that you put your "dirty coins" into, select a few options, provide receiving address(es), and receive "clean coins" from a separate stash. Mixing your cryptocurrency will mitigate the possibility of Blockchain analysis.

As for mitigating the off-chain analysis, just don't share addresses and other information pertaining to your cryptocurrency wallets on forums and whatnot. You just need to practice basic OPSEC here.

Cryptocurrency mixing service providers

In my article for AlienVault, I also made a list of things to look for in a mixing service provider, in addition to a small comparison spreadsheet of services.

Characteristics to look for in cryptocurrency mixing service providers:

- *"Data retention policy* – less logging is better, preferably none
- *Trustworthiness* – service provider has a good reputation in public forums, be wary of pop-up scam operations
- *Cryptocurrency support* – does this provider support my desired cryptocurrency? Most only support Bitcoin
- *Service fee* – the fee for service usage, random is better (1-3% is standard)
- *Delay* – the length of time that you delay a transaction from occurring, this helps privacy
- *Darknet or clearnet* – darknet providers are generally preferred since the operator is maintaining personal anonymity"

Part Six: Considering Operational Security and Mental Health

Dealing with OPSEC Burnout

> "Burnout is a political and movement issue. Every year committed activists suffer and drop out of our community because they have burnt out."
> (*Sustainable Activism & Avoiding Burnout*, Activist-Trauma)

This statement is true; after all, it took me years to finally release *this* very text that you are reading now.

What is OPSEC Burnout, and how does it affect me as an OPSEC practitioner?

Everything that we have discussed thus far may seem like common sense: if we want to practice operational security for our identities effectively, we must have goals, compartmentalization, avoid cross-contamination, and so forth. However, regularly practicing these things can be very exhausting. More often than not, I have found that people typically give up on independent underground operations requiring longterm OPSEC practices due to exhaustion, loss of time, and most importantly: *burnout*.

> "Burnout is defined, and subjectively experienced, as a state of physical, emotional and mental exhaustion caused by long-term involvement in situations that are emotionally demanding. The emotional demands are often caused by a combination of very high expectations and chronic situational stresses. Burnout is accompanied by an array of symptoms including physical depletion, feelings of helplessness and hopelessness, disillusionment and the development of negative self-concept and negative attitudes towards work, people, and life itself. In its extreme form, burnout represents a breaking point beyond which the ability to cope with the environment is severely hampered." (*Career Burnout – Causes and Cures,* Elliot Aronson and Ayalya Malakh-Pines)

In order to carry out an operation effectively, we need to be both physically and mentally up to par. Otherwise, we will deny our own needs, and "when we deny the vulnerable aspects of our nature, they can easily resurface in more problematic ways." (*Sustainable Activism & Avoiding Burnout*, Activist-Trauma) When these problems surface, they will more than likely negatively impact both our personal wellbeing and operational success. Never mind thinking that you must be busy 24/7 in order to find success; in order to succeed in your operations, you must maintain a healthy lifestyle.

In activism, research has allegedly highlighted that "burnout often appears to be caused by people setting themselves unrealistically high standards, which they are never quite able to meet, no matter how hard they drive themselves." (*Sustainable Activism & Avoiding Burnout*, Activist-Trauma) By setting unrealistic goals and taking on a great amount of responsibility, it will bring you down over time and, ultimately, burn you out.

In the case of hackers or other OPSEC practitioners, I have personally found that people often experience something that I'll be calling "*OPSEC Burnout*". OPSEC Burnout occurs as a result of the loneliness, self-discipline and excessive selfawareness over a long period of time. When OPSEC Burnout

occurs, an individual may find themselves not being capable of moving forward in their activities, and in many cases, destroying personas early and never meeting operational goals. This individual may also find themselves bringing down their co-operatives morale, and losing motivation to participate in activism and movements.

B3RN3D also acknowledges the issue of OPSEC Burnout in their article *"*Growing a Flower in the Dark,*"* discussing the drawbacks of issues relating largely to our loneliness as OPSEC practitioners. A realistic point that they make is that "depending on your OPSEC and operation, you are lonely. You sit in your cheap flat, with your secure computer, and nobody knows that you exist."

B3RN3D goes on to explain that loneliness for an OPSEC practitioner can breed from a variety of feelings: depression, laziness, myopic focus on the task at hand. Providing more insight, they explain that "when you have nothing else to do, you go to work. Take care of the operation. Plan, review, and plan some more. There's nothing else to do." However, doing this for too long will catch up to you, and ultimately you will burnout, and face issues in performing optimally – if at all.

Honestly, this is is my personal favourite blog of B3RN3D since it is all too real and the issue of OPSEC Burnout is not talked about enough in hacker communities. On that note, I will share a little anecdote about myself...

There was a time where I regularly wrote OPSEC blogs, maintained a variety of fabricated identities, independently researched privacy, national security and surveillance issues, and consistently stayed on top of my cyber life by participating in communities that required OPSEC practices. All was well, except that I had fully submerged myself in these activities for a long period of time, for years. This all caught up to me, drove me paranoid for months, I had become obsessed with my hobbies, and I had developed some very serious trust issues. In the end, I burnt out, destroyed nearly everything, changed my goals, and since then have lost a certain activist edge to me that I love.

You can avoid doing what I did by being realistic with yourself and by being aware of the OPSEC Burnout symptoms. As B3RN3D said, "[don't] only plan for the technical details, but also find ways to grow your flower in the dark." (*Growing a Flower in the Dark*, B3RN3D)

Knowing the symptoms of OPSEC Burnout

Look at burnout symptoms as a warning sign that you need to re-evaluate how you are managing both personal emotions and operational practice. We must acknowledge our own humanity, and remember that we have the right to pleasure and relaxation.

Some symptoms outlined by the *Sustainable Activism & Avoiding Burnout* paper include:

- A creeping feeling that [work activity] is taking over your life
- Difficulty in making decisions

- Inability to stay focused
- Insomnia, difficulty in sleeping, or getting enough sleeping
- A growing tendency to think negatively
- Pervasive feelings of hopelessness
- A loss of sense of purpose and energy
- Physical indications of burnout include muscle tension, restriction of blood flow to the tissues and increased adrenalin buildup. These physiological signs can lead to headache, backache, and exhaustion
- A loss of pleasure in food, friends or other activities that were once exciting and interesting – a general sense of running on empty
- Other warning signs of burnout include temper tantrums over trivial matters, not wanting to get out of bed in the morning or becoming accident prone

You can generally tell if you are burning out by an increasing feeling of being lonely, doubting your self-worth, and losing motivation. Your mental exhaustion will leave you also feeling physically exhausted and at a road-block in your operation. Look at burnout symptoms as a warning sign that you need to re-evaluate how you are managing both personal emotions and operational practice.

Preventing OPSEC Burnout

Preventing OPSEC Burnout can be challenging considering how *hush-hush* you must be with your operations, and will likely be feeling lonely no matter what. To combat OPSEC Burnout, B3RN3D suggests a few things from their experiences:

- "Meet people in an agnostic setting such as a book club, pub, or sporting event. Be weary of topics and information that are discussed but if you need human interaction, this is a good way of doing it."
- "Find an out-of-band low latency communication network. Connect to IRC or Twitter from an Internet cafe. Ensure you've compartmentalized everything properly and you're not using the same network connection as your main operation, but if you need to talk to someone."
- "Make a friend. Yes, this sounds simple or scary depending on the person but meeting a friend or partner you can confide in helps a lot. They might not be able to come over and visit you and you might seem like you're a very private person to them, but sometimes having a short conversation about the weather is all you need to remind you that you're connected to the rest of the world."
- "Attend a public event. I've found that even if I'm not interacting with people, being a fly on the wall at a very large event makes me feel less lonely. Even a bit of eye contact helps make you feel better."

- “Phone hotlines. I’ll be honest, I’ve never done this but a friend suggested it and swears by it. They suggested a suicide hotline but I feel that’s a bit crazy especially as these services are designed to track your location. Phone sex services are usually expensive too. If you can find some kind of free hotline service that lets you use your burner phone, maybe this is something for you.” (*Growing a Flower in the Dark*, B3RN3D)

B3RN3D also gives a few tips for upholding motivational efforts:

- “Start an operation, and write down exactly why you are doing this in the most detail possible. Yes, this is a risky proposition but if you can keep it secure, it can serve as an affirmation on the days when you’re questioning whether you should be doing what you do.”

- “If your operation is related to some moral or ethical motivation, review the reasons you chose to do this. Read articles and papers about what made you want to do this in the first place. If you’re a hacktivist, remind yourself of the bad things and why you’re trying to be on the good side.”

- “Limit outside influence. In contrast to the last suggestion, don’t read anything. Don’t let articles, comments, or TV shows suck out your motivation.” (*Growing a Flower in the Dark*, B3RN3D)

Bottom line, we are people, and people have needs. Satisfy your needs or you’ll crash and burn. At the end of the day, we must take care of ourselves, even if that means setting the operation at hand aside for a day or two. Believe it or not, your well-being actually matters.

Part Seven: Conclusive Statement and Additional Resources

Conclusion

This guide to applying operational security to your online identities has been a pleasure to write, especially for you cypherpunks out there. It is important that we have the choice to consent to what information is shared, and if we cannot consent, it is important that we understand how our information is shared. As a famous cypherpunk said, “we must defend our own privacy if we expect to have any.”

Over the years, I have created a lot of identities and accounts online. I have been lucky enough to learn through trial-and-error without negative experiences sticking to me too much. In my earlier years, I was always seeking digital privacy resources to learn from, but I could never find a thought guide to maintaining a digital identity. This is why I spent hundreds of hours writing this. I *wish* I had this thought guide years ago. I sincerely hope that this collection of thoughts is able to aid someone in a similar position.

If you are still interested in learning more about everything to do with operational security or security, I strongly encourage you to allow yourself to free your mind and do research on your own beyond this guide. I added a section for my recommended resources for further learning for those interested.

Again, it has been a pleasure writing this for people to learn from. This has been the first edition of *Privacy for Identities: The Art of Pseudonymity*.

Thank you for reading.

Recommended Resources for Further Learning

Title: OPSEC: Because Jail is for wuftpd
Type: Video, conference talk
URL: https://www.youtube.com/watch?v=9XaYdCdwiWU&t=53s
Description: This video covering hacker OPSEC is a necessary watch for anyone who is interested in the subject, especially hackers. The Grugq covers some very interesting case studies that allow you to learn from other hackers OPSEC failures.

Title: B3RN3D
Type: OPSEC blog
URL: http://www.b3rn3d.com/
Description: B3RN3D is a blogger that is well-versed with topics such as operational security, maintaining anonymity, and mass surveillance. I often reference this blog in this reading. B3RN3D, if you are reading this, thank you for sharing your thoughts over the years – I'm a personal fan of your work and would love to chat.

Title: GreySec Hacking Forums (Anonymity and Privacy forum)
Type: Forum board
URL: https://greysec.net/forumdisplay.php?fid=10
Description: GreySec is a community of hacker-oriented types, many of which have an interest in Anonymity/Privacy research, like myself. There are a lot of great threads on this forum worth checking out, and users with unique perspectives.

Title: The Paranoid's Bible: An anti-dox effort
Type: Resource repository
URL: https://paranoidsbible.tumblr.com/library
Description: Self-described as a "repository of knowledge meant to help people remove their information (Dox) from the web and people search engines." Excellent, credible resource for removing information about your current identity.

Title: Alpraking's OPSEC guide to being a successful kingpin
Type: Text guide
URL: https://pastebin.com/0CxYx1BD
Description: Alpraking is an experienced drug kingpin in the online black market. In this post, he describes how he manages people and his drug operation with respect to operational security. Without great operational security, he would not be in business. This piece offers fantastic perspective from the black market community.

Title: How to Disappear: Erase Your Digital Footprint, Leave False Trails, And Vanish **Type:** Book
URL: https://tinyurl.com/disappearing-frank (redirects to Amazon.com page)

Description: This reading focuses on the offline side of disappearance; Frank Ahearn, an experienced skip tracer, guides us in preventing skip tracers and other parties from tracking our trail. This is an interesting read for anyone whom wishes to conceal his or her real identity. Pro-tip: start by buying this book with cash and a hoodie in a brick-and-mortar bookstore.

Title: How to Lie to People: Achieving Anonymity through Disinformation and Data Poisoning
Type: Text guide
URL: https://pastebin.com/tXhiMk36
Description: DIzzIE provides helpful insight on how to lie effectively, and explains why and how lying can benefit your persona. This excellent resource can be read on your lunch break.

Title: OPSEC failures of spies
Type: Video, conference talk
URL: https://www.youtube.com/watch?v=BwGsr3SzCZc
Description: A case study on targeted surveillance. Explains how "telling" metadata is, specifically metadata pertaining to cellphone networks. This case study provides the opportunity to learn from the OPSEC failures of spies.

Title: How to Master Secret Work
Type: Text publication
URL: http://www.historyisaweapon.com/defcon1/secretwork.html
Description: Discusses the necessity of being able to carry out work and operations with assured secrecy. Governments subject to corruption have used dirty tactics to silence opposition parties in the past, and they will do it again. This resource will aid you in your thinking for illustrating underground operations in secrecy.

Title: No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State **Type:** Book
URL: https://www.amazon.com/No-Place-Hide-Snowden-Surveillance/dp/1250062586
Description: Glenn Greenwald is a leading journalist in terms of the Snowden revelations; he worked alongside Laura Poitras and Edward Snowden. In this book, Greenwald shares the story of him assisting Snowden with the NSA leaks. This book offers in-depth insight regarding the current state of surveillance and educates us about the surveillance tools that are utilized by the NSA.

Title: Citizenfour
Type: Video, documentary
URL: http://www.imdb.com/title/tt4044364/
Description: Laura Poitras and Glenn Greenwald meet with Edward Snowden in Hong Kong; Poitras interviews Snowden and Snowden explains the current state of surveillance in his own words. This video documentary goes hand-to-hand with Greenwald's book *No Place to Hide*.

Title: Centralised Place for Privacy Resources
Type: Blog, resource repository

URL: https://themanyhats.club/centralised-place-for-privacy-resources/
Description: A list of privacy resources and security technologies. Great resources, it is definitely worth checking this list out to get more familiar with modern day security technologies and pro-privacy solutions.

Title: Surveillance Self-Defense
Type: Resource repository
URL: https://ssd.eff.org/en
Description: Collection of resources, tutorials, and briefings pertaining to countersurveillance efforts. Includes tutorials for secure deletion, using PGP, OTR, 2FA, Signal, Tor services, etc.

Title: The Motherboard Guide to Not Getting Hacked
Type: Guide (PDF)
URL: https://assets.documentcloud.org/documents/4222455/The-Motherboard-GuideTo-Not-Getting-Hacked.pdf
Description: Generally good advice for security practices. Covers security basics, mobile security, privacy, messaging, and avoiding state and police surveillance.

Title: A Cypherpunk's Manifesto
Type: Manifesto
URL: https://www.activism.net/cypherpunk/manifesto.html
Description: A manifesto written for cypherpunk's by Eric Hughes in 1993. This is a very motivating pro-privacy read.