THE CRYPTOPAPER

PRIVACY, SECURITY, AND ANONYMITY
FOR EVERY INTERNET USER.

ABOUT THE AUTHORS

Crypto | Seb
Hello. My name is Joshua but many in the online world know me as Crypto | Seb or just Seb. There is absolutely no correlation between my name being Joshua and my alias being Seb (Sebastian). Simply put, I just didn't think using my name as an alias was all that cool. Back in 2015, some online friends and I noticed a gap in the information being provided to people to better their knowledge of security, privacy, and anonymity in our ever-changing digital world. We could find papers, forum posts, and discussion around little bits and pieces but we had to do the searching ourselves and put it all together. It really wasn't suitable for like 75% of the Internet population. So in early 2016, I had this idea of writing a paper that would encompass everything related to security, privacy, and anonymity but tailor it to all walks of Internet users; whether that is my 59-year-old grandma, or Edward Snowden like individuals. This paper, titled "The Crypto | Paper" resembles the beginning of my alias because it largely a collection of my own personal thoughts, knowledge, and experiences. As well, this paper is not going to be something that strikes every individual in a good spot 100% of the time – you WILL disagree with some of what is included and that is perfectly fine. We encourage you to submit corrections or give suggestions on how we can improve it. You can email me or hit me up on Wire (root@cryptoseb.pw) or follow me on Twitter (@CryptoSeb), to do either of the above.

Balockae
I decided about 55% of the way through writing that I wanted to bring someone in as a second part who would be able to provide their own input into what is largely a one-sided paper. This created some issues because I hadn't accounted for a second person or co-author so I was writing in first person. I would however, like you to meet Blake or @Ba_lock_ae on Twitter. We have been friends for a few months now and I figured he would be a great addition to the paper. So even though it has been written in first person (using "I"), some of the ideas and additions were his. I can't take all the credit – only about 85% haha. You can get in touch with him on Twitter or through email/Wire (perdite@protonmail.ch).

Reviewing / Content Editing
Originally, I had these high hopes for this paper to get peer-reviewed by some big(ger) name people in the privacy/security industry and even though many of them agreed to take on the task, lives are busy and the paper is 61 pages. So I am just going to have to settle with a little more harsh criticism from the public. I know there has to be places in here where I am dead wrong or you think I should add/take out something so I encourage you to really speak up if you see the need. I intend on publishing an edited version 1-2 months from the initial release.

A Brief Introduction

Reasons Behind The Crypto | Paper

Back in mid 2015, I (among other friends) started to see a real issue with the people using the Internet. Not only were they using it completely incorrectly on so many different levels, but they didn't have the resources to acquire accurate knowledge and change their behaviors. It isn't necessarily the fact that people want to use the Internet incorrectly, it's just that we have come from Windows 95, 50 pound desktop computers, 512mb of RAM, and Minesweeper, to petabyte servers, Google, self-driving cars, and ransomware in the course of 16 years. We have made technological leaps forward and it is literally consuming the massive portion of the population who weren't born/raised in this era or who don't have an interest in becoming "tech-savvy". And yes, consuming is the right word. I swear if a computer could eat you, some of the 65-year-old people trying to text their grandchildren would be gone. That phone would have a mental break down as they 'attempt' to use it correctly and just eat them.

But I have nothing against people who cannot seem to understand the security/privacy/anonymity aspects revolving around technology. That is actually the reason for this paper being developed in the first place. I want all my grandmas to be successful Internet users and not have to approach it with such a disconnect. Furthermore, we want avid tech people to also find a benefit and learn a little as well.

Uniquely Designed

Designing something of this magnitude wasn't as easy as you would think. I needed a way to separate the content so it had some sort of "flow" to it. But I also needed it to be something that wouldn't lose the less experienced people right off the start. The idea I came up with was the split it into 4 categories of people:

- Common Internet Folk
- Business & Tech Geeks
- Government Level Individuals
- Edward Snowden?

As you move up from one category to the next, the information becomes more intensive and techy. I hope that this method ensures adequate learning on behalf of ALL Internet individuals and we (Blake and myself) definitely encourage you to learn in the sections where you are lost. This is meant to be a tool of knowledge to promote your learning!

Common Internet Folk

What is Privacy?
Wikipedia describes privacy as “the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively” and I would largely agree that the definition provided fits the mold. However, I would suggest another definition as well. “Privacy allows everyone else in the world to see your life through a selective lens of your choosing.” It means to have the choice to not allow your neighbours to view your bank account information. It means only displaying certain information about your Facebook profile to the general public. And it means having curtains on your bedroom windows to conceal your sexual acts from onlookers. Privacy means keeping us safe…

Well Then What is Security?
… and security is what keeps us safe. Privacy is the idea; security is the thing. In the online world, security is what safe guards our information from hackers, thieves, Joe sitting next to you at the coffee shop, and even Government bodies who want a little more control. It encompasses a wide range of “things” that we use to keep our data compliant with the Privacy Rules we, or the organizations and services we use, specify. Security would be things like encryption, or strong passwords. Privacy would be not letting a coworker watch you type in these passwords.

Okay, So What About Anonymity?
Privacy and security are very closely related and anonymity is just the distant uncle who always shows up the party in socks and sandals. I say this because everyone makes fun of him at first, until it starts to rain and they all wish they had his nice warm wool socks on their feet to protect them. Anonymity is the concept of not being identifiable as your true self online. It seems to get a really bad reputation because a lot of hackers and online criminals are referred to as being anonymous. But it is also a very positive thing. Like in cases where a teenager who is questioning their sexuality wants to conceal their online activities from their parents or school until they are ready to make that big coming out moment. Or for a police officer doing undercover work to takedown a child pornography ring. Countless individuals around the globe use anonymity in some form or another every single day. As a final note, I think it is also important to understand that anonymity isn’t always just important for people as individuals but people as a collective. To have a truly open democratic system, anonymity plays a huge roll. It grants us free speech, allows us to question with negative repercussions, and gives us a means by which we have choice.

Let Me Explain Further...

Based on the arguments I have had with people in the past, I don't think simply explaining what security, privacy, and anonymity are will be enough for many of the readers taking a look at The Crypto | Paper. I think part of this comes from the mindset people have while using the Internet, but I also think part of it comes down to people just not knowing how serious the issue of privacy and security is. Let me give an extended explanation.

The primary reason for curtains/blinds/drapes covering our windows in our house is to stop people from being able to see in. The reason we don't want them to see in is because we consider much of what we do inside our homes to be private. Whether that be having dinner at the table, watching a movie with your kids, or even engaging in intimate or sexual acts with your partner. None of these things are illegal by any means but even knowing this, we still keep the curtains and blinds on our windows. We clearly have this strong desire for privacy when it comes to our personal life and the public. The same is true for our personal affects in not so personal places – like using an ATM (with your, personal, debit card) or paying with Interact at a grocery store (not such a personal place). It would be foolish to not cover your pin while it was being entered or to make sure the person beside you in line wasn't recording you while you entered it in. Even if we aren't consciously being safe about these things, our subconscious has our back most of the time. Think of this: If there were 5-6 rough looking individuals joking around by the ATM in the entrance of a bank, do you think many of the women looking to get cash out would be feel comfortable going in to do the transaction? Or do you think they might wait until the group left? In so many ways we have this consideration and desire for security and privacy but then we move into a digital era and really begin to harness the capabilities of the Internet and many of us just throw it all away.

It's hard to think of all the ways where we put our very personal information out into the world, while holding this belief that it "has to be safe. Just because." so here are some examples:

- Many Debit and ATM machines only use the 3DES encryption algorithm to keep your financial information safe. 3DES was developed in the 1970s and is the predecessor to the much more cryptographically sound AES algorithm. http://blog.erratasec.com/2013/12/target-displays-its-incompetence.html
- You pay for a catalog order by calling the company and telling them your credit card number over the phone. The representative then reads the number back to you for verification.
- You keep an agenda book in your purse with your passwords written down in it.
- You use the same PIN to unlock your phone that you do with your debit card or credit card.
- You use the same email for your online banking, PayPal, iCloud (important accounts) that you hand out to the cashier when asked while out shopping.
- You have texted someone a password, piece of financial information, SSN/SIN.
- You use less than 5 different passwords for everything online.

I would have liked a way to record people's facial reactions while they read the bulleted list above. I am curious to know how many of you went down all 7 items and said quietly to yourself "yup, I do that too". But these typically aren't things we consider to be insecure. You deleted that message you sent to your husband with your social security number in it so you must be safe, right? Not quite. The digital world is so vast and is comprised of numerous "levels", for lack of a better word. You as an Internet user would be one level, a system administrator doing work on your bank's server would be another level, your bank itself would be another level, the people setting rules and regulations for that bank another, and high level government organizations are usually the final level at the top. So even something so simple as logging into your bank account has the potential to hit tons of these "levels". This is both good and bad. On one hand, it means our information is being looked after by a varying amount of people, companies, and organizations – no better way to determine the faults in our security. But on the other hand, HOLY SHIT! OUR INFORMATION (that we probably want to be private) IS BEING LOOKED AFTER BY WHO KNOWS HOW MANY DIFFERENT PEOPLE, COMPANIES, AND ORGANIZATIONS. You wouldn't likely walk outside to go to work and tell your neighbor "Yup, had some really great sex last night with my fiancé!" But… you would text that to a best friend over SMS where there is a potential for one of these people or organizations to have a little peek at it?

The NSA (National Security Organization) has been running a program called Dishfire that collects up to 200 million text messages per day from users globally. For reference see here: http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents, here: https://en.wikipedia.org/wiki/Dishfire, and here: https://secure.link/4NSuQHGs

This means that the text message you sent your buddy about the wonderful sex, could have been read by a member of either the NSA or the similar GCHQ in Britain (whom they have granted almost unrestricted access to Dishfire data). Think about that for a second. Someone you don't even know, from a country you may have never even have visited, knows about your sex life, all because you texted it to a friend. This is just the beginning too! The NSA has been rumored to have a program capable of crawling the Internet and mining (collecting) mass amount of data for later analysis. Due to the classified nature of really anything the NSA has in its possession, we obviously don't know what information, or how much information is being gathered (if any at all) but based on the size of the NSA datacenter (https://nsa.gov1.info/utah-data-center/udc-photo.html), I would say an astronomical amount containing the sum of EVERYTHING. You don't have a data center that large without a purpose.

If it doesn't concern you that a member of your government is able to see everything you are doing online, read the text messages you are sending, or even listen in on the calls you are making, it should scare you to know that companies like your Internet or mobile service provider likely have the capabilities to do this as well. See: http://hotair.com/archives/2015/08/16/attverizon-nsa-partnership-shows-why-government-and-businesses-shouldnt-mix/ and http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

“But they are just doing it to keep us safe! And besides, I have nothing to hide!” – These statements are valid for you to make, but really based on false ground. Think about the argument I made earlier concerning the blinds and curtains in your house. They keep you safe and allow you to go about your daily lives in private. Not that we are being secret about any of our life, or that we close the curtains just so we can commit illegal acts, we simply use them because we don’t like the fact that someone walking by at night could see, watch, and even record everything we are doing. Imagine what it would be like without those blinds. Would you still feel comfortable engaging in many of the same activities that you do? Would you still masturbate in your bedroom where the neighbours had plain view from their kitchen window?

So if we aren’t going to give the public ready-made access into the details of our daily lives, why are we making an exception for our governments? Because technically, the same governments we are making exceptions for, are made up of these individuals from the same public who we do not want knowing and seeing this information. They are people with whom we can’t verify the intentions or motives of. They could be watching your every move (with or without the consent of their superiors) and you would be clueless. The same goes for the individuals in the same room as the lady you read your credit card information to while making that catalog order over the phone. Was there someone else in the room with malicious intent writing down the number, expiration data, and CVV code while this representative read it back to you for “verification”? I guess you’ll have to be okay with the fact that you will never know.

This is why privacy and security matter. This is why we need to implement strong encryption and NOT let anyone have a backdoor in the code. Although we may have good intentions as individuals, we can’t rely on the assumption that other individuals will have good intentions as well. If we do not hold the companies who are storing our personal information (like our bank, PayPal, Facebook, etc) accountable and responsible for keeping our information and identify safe, we will willingly be moving into the unknown. Into a digital era where it is more common for a random onlooker to know more about your personal life, financials, and account information than another member of your family. Mozilla put it best: Privacy Lets You Be You. https://advocacy.mozilla.org/encrypt/social/1

So keep this in mind when you are reading the remainder of this paper. I didn’t do a lot of explaining with precise examples as to “why” you need the security, privacy, and even anonymity as showcased in the next 50 pages… but it shouldn’t be rocket science. We can’t really assume that backdoors, government surveillance, and poorly developed security measures are keeping us safe just because we trust the people using and implementing them, can we? If so, take a look at this breach that compromised 20,000 FBI and 9,000 DHS employees and imagine how secure your life would be if you left it in someone else’s hands: https://motherboard.vice.com/read/hacker-plans-to-dump-alleged-details-of-20000-fbi-9000-dhs-employees

Watch: https://www.youtube.com/watch?v=VPBH1eW28mo. It explains locks + technology.
Watch: https://www.youtube.com/watch?v=V9_PjdU3Mpo. It explains mass surveillance.

Defining Your Threat-Model

For starters, a threat-model could be defined as how an individual needs protected based on things like: the valuables they own, the information they know, or the work they do. Someone like the President of the United States is going to have a much greater threat model than someone who works at a grocery store. However, this doesn't always apply to the Internet world because we often don't look at the idea of threat modeling from a holistic approach. We tend to see it as good guys VS bad guys when it comes to the whole security, privacy, and anonymity concept. Think of someone like Edward Snowden – the big whistleblower that revealed a ton of NSA secrets regarding the privacy of US Citizens. His threat model is very different from yours or mine because his life is literally on the line. People want him dead for what he did. So before diving into the whole idea of security, privacy, and anonymity in the online world, we need to ask ourselves: what and who do I need protection from and what information or data are they going to try and get from me? See yourself as a storeowner and assume that someone is always going to be trying to take what you have and use it for his or her benefit. This is where the idea to break this paper into 4 sections came from. We go from common internet folk, to tech savvy users like myself, to government officials, advocates, and the like, to Edward Snowden himself. Once you have determined whom you need protection from and what you need to protect, you should be able to take the steps to further your knowledge and stay safe online.

Encryption. EVERYTHING ENCRYPTION.

I am a pretty big believer in encryption online because generally, encryption is the primary tool that keeps our information/data secure. It prevents outside people from taking a looksee at things we would probably like to remain confidential. Wikipedia defines encryption as "the process of encoding messages or information in such a way that only authorized parties can read it." With this tool available to us in so many different forms online, we are foolish to not make sure a huge portion of everything we do on the Internet is encrypted. We should be encrypting our computers. Encrypting our connections to websites. Encrypting our communications. Encrypting the places we store confidential information. Even encrypting our search results on Google. I believe that this is how we are going to be the most secure in this digital world – by making all this data unreadable to anyone that we do not specifically grant the ability to read. Sort of like the lock on your front door. Without a key, people don't get in unless they use force. And the stronger that we build our house, the more secure our door is, and the bigger fence we put up on the outside, the harder it is to use force to gain entry.

Firefox Please

Diving right into the specifics, I want to start off with the most common mode of accessing the World Wide Web, your Internet browser! Probably around 99% of the people reading this are using it right now (unless you are reading a printed out version of course). The most common examples of a browser are: Internet Explorer, Safari, Chrome, and Firefox. Ideally, you want to be using a browser that is being developed by a company who is dedicated to your security and privacy in the online world. It is also considerable to use one that doesn't inhibit your browser experience by flooding you with options. It should just make your experience secure/private in a seamless fashion. For this reason, I recommend Firefox. It is open source, and widely used by

security professionals. It is also very secure and enhances proper usage with little things that are easy for individuals to pick up on while still being very customizable to those looking for something more. It has a feature called “In Private Browsing” which doesn’t log your history, store permanent cookies, or save search results. You can also download “Add-Ons” that both tailor your browser to your needs, and offer more security. As a side note for those individuals looking for a really high level of security, privacy, and anonymity, Firefox is also the base that the Tor Browser is developed off of, which I would say is a very good argument for using it as a daily browser.

HTTPS / Browser Encryption

Often times when you connect to a website, you will notice that the URL just displays the website name (ie: amazon.ca or www.amazon.ca) But as we move into a more digital world, it is highly recommended that sites use SSL Certificates and Transport Layer Security to encrypt your connection to them. This displays in your browser as https:// with the S being the important thing to look for. Now, browsers like Safari on your iPhone/iPad/iPod and Firefox on your desktop/laptop are making it easy for you determine which sites are secured and which are not by displaying a lock icon beside the website. See this linked example of PayPal’s website that shows not only the lock icon, but also identity verification known as an Extended-Validation Certificate (green words beside the lock) to supply a trust factor in making sure you are connecting to the real PayPal website http://prntscr.com/amwib2

In a nut shell, when you connect to a website with an SSL Certificate, it means that everything you do in association with that website is going to be encrypted from your browser, to the website’s server, and then back to your browser. This includes login information, passwords, financial information, and all other personal details. Even on my website cryptoseb.pw, I have an SSL Certificate that is using TLS to encrypt all the traffic. I don’t have a need for one at all, but it is good practice to always use one. Encryption is never a bad thing on the Internet. But be careful, certificate authorities can and have gotten hacked/breached in the past, which would compromise the security of every certificate they have issued. HTTPS doesn’t just provide us with encryption for the data in transit either. It gives us a way to authenticate the data. With a website transmitting all the information over plaintext, you can’t be certain that even the website you are viewing is the real one. If your connection was victim of a man in the middle attack, the data could be compromised at any time. This is not an easy task when a website makes proper use of SSL/TLS.

However, encryption to and from a website isn’t always up to current standards and can be misconfigured, using weak algorithms/cipher suites, or have trust issues with the certificate. The best way to find out if the website you are connecting to has good stats on their certificate is to head over to https://www.ssllabs.com/ssltest/ and put the website URL into the scan box. I have configured cryptoseb.pw to get an A+ with complete 100s down the list. This is serious overkill and loses support from some older browsers, but it means the highest level of security. Here are some pointers on what to look for to acquire maximum encryption strength/trust:

- Certificate is TRUSTED
- Key is greater than 2048bits (RSA)

- TLS1.2 offered as a protocol but NOT SSL
- RC4/MD5 ciphers are NOT allowed server-side
- Secure Renegotiation enabled
- HSTS Strict Transport Security enabled
- Public Key Pinning (HPKP) enabled
- OCSP Stapling enabled
- Forward Secrecy enabled

Choosing and Using Strong Passwords/Passphrases
Now, there is a difference between some terminologies here that seems to be used interchangeably when they aren't really the same.

PIN – Numeric characters in sequence (usually 4 characters in length)

Password – Letters, words, numbers, spaces, and symbols in sequence

Passphrase – Significantly longer than passwords often with words in sequence

Passcode – Apple's take on a PIN/Pass combination (usually 4 digits but alphanumeric option available)

So when we take a look at creating passwords that are secure enough to protect us online, people tend to have the assumption that your passwords have to be all random characters and all different from each other. What a nightmare to remember! This isn't true for like 97% of the population. Your passwords should be, for the most part, all different, but they do not have to be a combination of randomized characters. Take a look at this diagram I did up on how to come up with easy to remember but very secure passwords:
https://cryptoseb.pw/passwords.png
This allows you to create passwords that you won't forget (as you only have to remember the base and the part being changed for each site) but keep you secure. You could even write down the part that changes somewhere fairly secure, like your Notes app on your phone. Even if your kids are snooping through those notes, you don't have to worry because they don't know the base you have created. From the example picture, you would be writing down grip = Facebook, toes = PayPal, etc

I would however recommend that instead of storing passwords on pieces of paper beside your computer, or in a diary you keep in your purse, or even on notes inside your mobile device, you look at getting a password manager like LastPass, Dashlane, or 1Password. I personally use and recommend LastPass for keeping all of your account information secure but easily accessible. It offers very good usability across your devices, and is accessible from anywhere in the world through your vault at LastPass.com. When you create an account, you are also creating a vault in which your passwords are stored. This vault is always encrypted on their server and is only presented in an unencrypted form to you from within their app, or in your browser after inputting your account information to decrypt it. All of this encryption happens behind the

scenes and is seamless with your login. They also have enhanced security features like Two-Factor Authentication, geo-location (country) restriction, and email security notifications. However if you fall into the last 2 categories of this paper I would not recommend storing passwords in LastPass for accounts that can be accessed with a warrant. Things like your SpiderOak account do all the encryption client side and they do not store your password or encryption keys server side. So storing this password in LastPass could present itself with some issues if someone was able to provide a warrant to get in and see all your passwords. You could still store parts of these passwords in your LP Vault but in a secure fashion to simply remind you if you are forgetful. Say your password for SpiderOak was "Koala_PURPLE-2015==", you could save the password in your vault as Ko*******5==. This should be enough to jog your memory, but not enough to give someone immediate access. For a yearly subscription to LastPass Premium, I paid $12, which is really affordable. I would link my referral code but I feel like that takes away from the idea that this paper is designed to be completely free and open.

Hashing & Authentication

It is important when we learn about encryption and using it alongside strong passwords, to also take a look at how these passwords are stored on the website's server. The issue is that once you send something to a server, it is out of your hands unless you operate the server yourself. So it is important for server owners to be storing as little information as possible on the server unless it is in an unreadable, encrypted format. SQL injections and database compromises can expose anything in plain text and they are surprisingly very common occurences. Hashing is similar to encryption but comes into play when securely storing password. When you register for many websites, they take your password and they store it on the server so that every time you login, it just compares the two passwords and if they are the same, it logs you in. However, this is incredibly insecure even with SSL implemented. The good websites/servers (which should be the majority of them now) hash your passwords before sending them to the server, which basically means storing them in a jumbled fashion. It is done commonly through what we call "hashing algorithms" like SHA256 or SHA512. As a side note, those are two common hashing algorithms that are often accompanied by PBKDF2 (which is used for key stretching https://www.schneier.com/cryptography/paperfiles/paper-low-entropy.pdf to thwart brute force attempts). Then we you login the next time to the site, your browser converts the password into that same string of random characters and matches it with the string of random characters it has stored on the server. If the two match, you are authenticated and allowed into your account.

Going into a little more detail on key stretching and PBKDF2, there is a related term known as Password Iterations or Iteration Count that defines the computational power that needs to be exerted between password attempts. The higher the number of rounds used, the more secure your account/encryption/password is going to be. Companies can also add a salt to the hash, which adds a random string of characters to the end that actively thwarts dictionary attacks (https://en.wikipedia.org/wiki/Salt_%28cryptography%29). For some reference, the default iteration count for 4 common services/applications are listed:

- LastPass – 5,000 (Client side) + 100,000 more (Server Side)
- TrueCrypt – 1000

- VeraCrypt – 500,000
- FileVault2 – 41,000

What Information and Where?

So once you have the basics of how the Internet can work with you to keep you safe, it is vital that you determine what information you are putting out there, where it is going, and who is able to view it. Everyone has seen the posts on Facebook where someone uploads screenshots of a text message that was clearly meant to be personal but somehow got leaked – likely from another party with malicious intent. It sucks to be that person getting exposed! So we must be careful with the information we are sharing and how it can be used against us. The general saying is that once it is out on the Internet, it is impossible to take it back or erase for good. One should always assume that something, or someone, somewhere, is archiving that information for later use or reference.

To start, take a look at common websites like Facebook, Instagram, Twitter and what privacy options they provide. Take Twitter for example. You can either protect all your tweets, or have your entire profile open to the public. This is the same with Instagram where your account is either entirely private or entirely public. Unless you are very selective with what you are posting, I would recommend having these privacy features enabled on both. The exception to this would be if you were very avid in the online world, famous, or running a business where the publicity from you posting is going to drive customers. For average people just posting about their personal lives, keep it locked down for security. It protects you from random onlookers and also from someone who may be trying to steal your identity. Facebook is a much larger mode of social media and encompasses a greater aspect of your identity so it is of course going to be more complex. But ideally, you only want the public to be able to see information about you that isn't personally identifying or revealing. An example of this would be your date of birth. People outside of a small circle of family and friends don't need to know that. Especially the people you meet on Facebook. This is why Facebook provides a bunch of different options on who you share information with. I generally only use the 3 common ones: Public, Friends, and Only Me. Things like my date of birth, email address, phone number, and sexuality are all kept to Only Me because they are things I don't want anyone else knowing unless I specifically hand it out to them. The majority of my other information is kept at the Friends level and only miniscule information is actually viewable by the public.

If you are one of the people who are relying on privacy, security, and anonymity to keep you safe, you should consider not using social media like this or being incredibly restrictive on what you are posting. All of these websites log your information and may even store it even after you delete it. Using dis or false information in these cases will benefit you. If you are very keen on using something like Twitter, maybe consider not using your real name and personal email upon registration. You must also take in consideration that these websites may not be keeping the information for just themselves to look at. We would be foolish to think they aren't selling our information out to third parties or handing it over to Governments when they ask.

Business & Tech Geeks

A Starting Place

I often times see people whom are clearly business people doing business related things with customers, clients, and the like in very public places in very insecure manors. I was just in an airport where a medical professional of some sort was discussing personal things with what I assume was one of his patients not 5 feet away from me. It was rather disturbing to listen to him as he wrote things down on a clipboard and I could hear the entire side of his conversation from 3-4 seats away. The nature of his call wasn't disturbing… but the fact that the person on the other end was having their privacy completely compromised was. What got even scarier is while he was finishing up the conversation, he asked for this person's health card number so he could document the conversation when he arrived. Not only did she give it to him over the phone, but he READ IT BACK to her over the phone. I could have recorded the entire conversation and I would have had her first name, and health card number along with a slough of medical related information about her. That is scary…

Take a look around next time you are in a coffee shop or public place like a library where people are using their laptop or tablet openly and see what they are doing. You may honestly be able to stand over their shoulder and watch them from 2 feet away for some length of time without them even noticing. These are places where people might even do financial transactions, update banking information, or send confidential emails/messages to clients and we are able to see it all as a passerby.

Securely Transmitting Information (Messaging/Calling)

Currently, technology allows us to communicate in so many different ways with each other that even 30 years ago we were unable to do. Skype, Email, Texting, Facebook Messenger, Twitter Direct Messaging, Mumble, and TeamSpeak are all examples of ways in which we communicate through technology. However, these are all methods of communication that are either inherently insecure due to the way they have been developed, or not used securely on behalf of the user. A study done by Forrester (http://blogs.forrester.com/michael_ogrady/12-06-19-sms_usage_remains_strong_in_the_us_6_billion_sms_messages_are_sent_each_day) claimed that in 2012, around 6 billion text messages were sent in the US each day. Those statics are 4 years old now but should give some insight into the usage of technology in this day and age.

Now, I want you to think about what you would message one of your friends or family members or what you have messaged them in the past. I'm not talking the day mumbo-jumbo either. Think about the times when you have said something really personal. Maybe shared a password with your girlfriend, took a picture of a bank statement and emailed it to another family member, or even sent your social insurance number to a future employer. These are all too common in the daily world of technology and it is incredibly foolish and negates the security of our identity on many different levels. Facebook, Yahoo, Google… they don't need to know this sort of information about you; even if they are claiming to keep it safe from third

parties. To add some more scary information to the mix, the National Security Association (NSA) in the US, runs a program called Dishfire (https://en.wikipedia.org/wiki/Dishfire), which collects hundreds of millions of text messages per day. How this is even a thing?

This is where companies like ProtonMail, Wire, OpenWhisperSystems, Apple (iMessage/Facetime), and Tutanota come in. They provide services that are dedicated to helping us communicate securely and privately with others. Most companies that WANT to keep you secure online will do so without draining your pocket either. Let's take a closer look at the first four listed above which are my go-to services every single day.

ProtonMail – Secure Email in Switzerland

Before coming across the ProtonMail crowdfunding campaign, I was an avid user of email services like Yahoo and Gmail. However, these services were only putting in a minimal effort to keep me safe. ProtonMail however, was marketing itself as the all-inclusive solution for encrypted email. Based out of Switzerland, ProtonMail providers end to end encrypted email that keeps your communications private. It is free, open source, and they have zero access to user data.

ProtonMail also employs some great security features that actively work to keep both your account safe, and your communications completely private. The first great security feature is the use of two passwords in the login process. The first password accesses your encrypted mailbox and the second password decrypts it. There are ways to employ fully encrypted email without using a dual password method but I prefer typing in two different passwords every time I log in. This allows me to store the first password in my LastPass Vault and the second in my head. Even if someone gets into my LastPass account, they aren't getting into my email. Another feature I really like is self-destructing emails. This allows really sensitive communications to take place within a set period of time, thus reducing the chance of them getting leaked to an unwanted party. Alongside this, ProtonMail allows you to encrypt emails to users who do not have a ProtonMail account using their secure reply feature. This gives us a chance to sort of impose the level of security we want on those we are communicating with. Lastly, ProtonMail now also offers the ability to link your domain name with your account and upgrade for premium features. This gives us a chance to use our own domain, which provides trust to those we communicate but does it all through the ProtonMail servers making everything fully encrypted. My email for my domain name 'cryptoseb.pw' flows seamlessly through the ProtonMail servers and provides me with a more secure email for communication, while giving me the benefit of keeping my online persona "findable" and tailored to me.

Wickr – The Most Trusted Messenger In The World

Previously, I had written quite the lengthy review here about Wickr and why I had been a dedicated user of the app for over 3 years. However, in July of 2016 I started using another secure messenger called "Wire" and shortly after, messaged all my Wickr contacts explaining that I would not be using it as a service anymore. Wickr is now fully fazed out of my communication channels. The reason for this change was simple. Wire offers everything that Wickr did (except ephemeral messaging) but on an open-source level. If you would still like to

read about Wickr and why it struck me as such a great company for over 3 years, it will still be available in the version 1 PDF file on my website. It was a great messaging app that I believe really paved the way for other services like Wire, but there refusal to open-source the product meant we as a user base couldn't verify their intentions completely; something that I described more in-depth at the beginning of the paper as being a no-no.

Wire

Replacing Wickr in what seems like a plethora of secure messaging apps and services that I have tried out is Wire. Wire is a company based out of Switzerland that was founded in 2012. I don't have much information about the application before the huge kick it had in July of 2016 when I decided to start using it, but I do know that for like 2 years it wasn't open-source and didn't provide many of the features it does currently. On the opposite end of the spectrum to my reference above, because Wire is open-source, we can validate the intentions of the developers and administrators behind the app on a greater scale. They would have to put some serious work into designing a backdoor to hand over information to an agency like the NSA considering the app is reproducible with the OSX and Windows versions.

Unlike many of the other apps in its category however, Wire is jam packed full of features and seems to be listening to user suggestions and really pushing out updates with new content on a regular basis. In the last 3 weeks since installing it, I think I have seen 4 new features that I found useful alongside getting open-sourced completely in that time (https://github.com/wireapp/wire). Some of the bigger features that Wire has going for it are:

- Messaging that is end-to-end encrypted and forward secure to thwart big data compromise from man-in-the-middle attacks
- Group chats with up to 128 people that are also end-to-end encrypted and forward secure
- Encrypted audio (group as well) and videos calls
- Support for encrypted attachments, photo sharing, GIFS, drawings, voice changing on audio messages, sending your location, and pinging other contacts
- Fingerprint verification
- Multi-device encrypted pushing so you receive all your content on all your devices
- Registration with either an email, phone number, or both
- Phone number is not viewable by other Wire users or by the Wire Server and email is viewable to both. This provides a layer of anonymity over Signal and allows a user to share their email linked to Wire for discovery

Wire provides both a Privacy and Security Whitepaper which are viable on their website at: https://wire.com/privacy/ and give in-depth analysis of how the company operates and how the internals of the application work. The only downside to the encryption used by the application is that it is sort of a knock of version of the current Signal Protocol. The developers of Wire took the Axolotl implementation and modified the ratchet calling it 'Proteus" and using it strictly in Wire. The basics of encryption are ChaCha20 for the stream cipher, HMAC-SHA256 as MAC, and Curve25519 for the key exchange. Should still be considered secure encryption by anyone's standard. For encrypted audio calls, Wire uses a mixture of HTTPS for call signaling

and SRTP-encrypted media sessions. Keys and parameters are negotiated through a DTLS handshake. You can find out more about the encryption used here in their security whitepaper.

It almost seemed to good to be true when I first stumbled across the app and not a week later they had open-sourced everything. At a glance, it might seem like Wire provides everything a user could ever want in a secure, private messaging app but it does have some flaws that could be improved upon. The first of which would be the support for ephemeral messages. The idea that a message is self-destructing and is not viewable by either party after a certain amount of time gives both parties the confidence in being able to discuss whatever they want without restrictions. With Wickr, all I needed to do was set a 5-minute destruction time on sensitive messages and I greatly decreased my chances of that message being stored for later reference. The second big thing I would like to see improved upon is the general UI of the app. Because Wire is packed full of features, it seems pretty hard to navigate on the iOS version if you aren't very tech-savvy. It took me about half an hour to show a good friend how to properly use the app, find others via their email address, and initiate chats/calls with them. Had to completely leave out the more advanced features like fingerprint verification, device management, and password changes because it was just too difficult for him to take in and navigate on his own. This wouldn't likely be an issue for others like me who have the experience to generally just pick up a new app and go, but it would still be nice to see a more user-friend interface. I am certain this will come with time as the application grows and moves forward. Lastly, it would be great to see a dedicated Linux application for Wire. I personally do not use a GNU based operating system on my primary computer but I do have quite a few friends that do. There has been talk that one is "in the works" so I am hopeful. Using the web version is not practical on your everyday OS.

I am very happy with the direction that Wire is going and really proud to say I would prefer this mode of communication to anything else currently in the abundance of secure communication methods out there. The support is wonderful, they are very active with their followers on Twitter, and give me the biggest vibe that they truly care about our privacy in this ever-changing digital world.

Signal – by Open Whisper Systems

Open Whisper Systems had originally created separate apps for encrypted calling and encrypted messaging called TextSecure and RedPhone back in 2010 but they have since combined the two services into one app called Signal. Signal is marketed on the Open Whisper Systems website as "Privacy that fits in your pocket". They are the encrypted texting and calling application used by many and advocated for by big name people in the security/privacy industry like Edward Snowden, Matthew Green, and Bruce Schneier. This really gives the application a level of trust that goes beyond its competitors in the same field like Wickr, Telegram, WhatsApp, or Facebook Messenger.

Signal is very simple to use and provides a level of encryption that is top notch A+ grade and usable for all kinds of conversations. It is also open source, which allows everyone to view and validate that the application is working exactly as it is being marketed to work. This also

provides transparency in assuring that the intentions of Open Whisper Systems don't change or become malicious. The one thing that Signal provides that is above and beyond Wickr is support for very simplistic encrypted calling. This means you don't have to just message someone, you can hold audio conversations with them completely encrypted and private from all levels of adversaries whether that be hackers, your mobile service provider, and even government bodies.

There are a few major downsides to the way Signal operates however and it definitely isn't for everyone. The biggest downfall of Signal is that it requires your phone number to operate. Even though they send only hashed phone numbers for contact discovery and uses encrypted bloom filters for calling contact discovery, this only prevents their server for seeing sensitive information like your name or number. But because it requires your phone number, you lose a serious level of anonymity over using something like Wire that does not explicitly need your number. Not everyone you have to speak with is going to be worthy of having your cell phone number; it is something that can compromise one's identity and lead to things like fraud and identity theft. This is especially true for those who rely on being anonymous in many aspects of their life, like journalists, activists, or even whistle blowers (Edward Snowden). I find it odd that a person like Snowden, who would likely need a very high level of anonymity in who he holds conversations with, uses a service that requires him to give up that anonymity with a cell phone that could be linked to his true identity. Another potential downside is that Signal does not give sender security in deleting the messages. Now, it is true that the idea of sender based security is sort of based on a false ground as it is nearly impossible to stop someone from recording or keeping a message if they are truly determined to do it. But, having messages that go kaboom and are irreversibly deleted is definitely better than allowing them to be stored on each device indefinitely.

Regardless, of these design flaws Signal is secure and that is what many people are looking for. It allows us to hold private conversations with another party in a fully encrypted fashion that keeps each party secure from anyone outside of said conversation. Signal isn't anonymous by any means but for many, that isn't an issue. I have started using Signal on a daily basis to talk with friends and it is starting to grow on me. You just can't beat the simplicity.

iMessage

Apple has provided a messaging service since the dawn of the iPhone many years ago and expanded on it to be a very privacy conscious and secure way of communicating. Now, nearly every person who has an iPhone, iPad, Mac, or iPod Touch uses iMessage. What hasn't really hit the spotlight and been discussed is the fact that messages sent iPhone to iPhone that show up as blue are sent fully encrypted end to end. When you first start using iMessage, your device creates two sets of private and public keys: one for encrypting and one for signing. Your private keys never leave your device, but your public keys are sent to Apple's servers to be used by others whom you communicate with. iMessage uses 128 bit AES for encrypting the messages and ECDSA keys using a 256-bit NIST curve for signing. This ensures both the authenticity of the messages and the strength of encryption is maximized. However, Apple does this fluently and the user never has to worry about enabling extra features or downloading other applications

like Signal to make this work. The only issue with iMessage that will hopefully be addressed soon by Apple is that the key servers are located in the United States. If they really wanted in, Apple isn't going to be able to stop them at this stage of the game. A good step forward would be for able to separate the signing keys into say 3 different geographical locations around the globe to maximize the effort needed for a full compromise.

Recently as well, Apple has begun encrypting device backups to iCloud using your device passcode, which means if you are using a strong enough passcode to protect your device, you are also keeping that same security across the board when your phone uploads its important data to the cloud for backup.

Storing & Sharing In The Cloud

Right alongside messaging people in a secure manner, we have to think about how and where we are storing files in the cloud, and how those files are being shared with others. Likely the most common forum of storing files and data in the cloud is to use a service like Dropbox, Google Drive, Mega, One Drive, or the like. Most of these services have been developed to keep the user safe from account compromise – allowing two-factor or step authentication/verification to keep everything locked up. Google Drive would be my top pick of the above for account security as they manage millions of accounts every single day and have quite the automated system for authenticating and fighting hackers/jackers from compromising your account and stealing your sensitive information. They make use of things you know and things you have, like your password and your cell phone to block unwanted access.

However, the thing these services don't do is prevent more powerful bodies from accessing your information and peeking in on the things you are storing with these services. Say you decide to store a Microsoft Excel document that you use for keeping track of all your financials inside of your Google Drive account. This file would not be encrypted on their server in a manner that only you could decrypt and could technically be viewed by anyone with enough credentials or clearance. This includes a government entity with a warrant. However, the majority of the population isn't defending themselves against large entities like that so Google Drive is a fairly good solution for many of us.

But… What if…?

The question stills remains on whether the average, ordinary person needs more security than what these services provide. I am an advocate for our privacy and a believer in encrypting everything we do online, so I would say yes! Because we can't account for all the "what ifs" in the world, but we can eliminate a large chunk of them. There are services out there that provide complete security of your files with strong encryption. These services give us full control of our files in the cloud and keep them secure from even the company being able to snoop on them. I was and still am a user of ownCloud, a service that lets you host your own cloud-based storage. However, it isn't encrypted in a manor that keeps files at top-level security so I ended up switching. There is also room for question on whether just encrypting your sensitive information gives an adversary knowledge of what to target. If the majority of what

you do online is in a plain-text manor, does that make your encrypted data more susceptible to attack?

Tresorit

The switch I made was to a company called Tresorit. They are a cloud service that takes file storage to a very desirable level of security. Everything you upload to your Tresor is encrypted device side before hitting their server, which means you have the assurance that no rogue system admin is going to be looking through your sensitive data. Your Tresorit password acts like the master key for everything you upload. Without this password, your files are irretrievable and lost in the cloud forever. This is good because it means no password resets and no compromised accounts. However, we technically can't verify this information as customers/users because Tresorit isn't open source. For those of us just looking to make a switch to something more secure, this isn't an issue. Tresorit is still encrypting all our files client side and presumably keeping the keys for the encryption and decryption process off their severs which is enough. But if you are the next Edward Snowden, I recommend looking at something that is FOSS (Open-Source). This would give you the comfort of having everything stored in your cloud service completely encrypted and would give you the ability to verify this through their published code. You can view Tresorit's Security Whitepaper here: https://tresorit.com/files/tresoritwhitepaper.pdf to read up more on the security they are employing to keep your files safe.

The Great Extras of Tresorit

I like it when companies offer more than just the basic product they are out to provide. Tresorit is a cloud storage service. It would be very easy for them to just provide secure cloud storage and call it a wrap. But they strive to offer more, which is a bonus for their customers. Probably the best added feature is being able to send encrypted links to download files stored in your Tresor. This allows a user like yourself to send someone else (whether a Tresorit user or not), an encrypted copy of the file to download. It remains completely encrypted the entire way to their browser. You can define an expiration time for this link and a premium user also has the option to set a password for the download. This is a big security enhancement over sending the file non-encrypted via email or another upload service. Another feature that improves the usability is being able to share Tresors with people. So I as a user could create multiple Tresors and upload different things to them (one for work, one for family, one for personal stuff). Then you can share those Tresors with respect people added as a contact on your account; granted they too have a Tresorit account.

SpiderOak

Although I haven't used SpiderOak, it is the open source alternative to Tresorit so I do think it needs a spot in this paper. They are a similar service to Tresorit and hold true to the zero-knowledge system that cannot be attacked from within to hand over data to law enforcement. They are also "Private by Design and Choice", a term you will see explained further on in this paper. The biggest benefit of SpiderOak over Tresorit is that it is open source and that should be very appealing to a wide variety of people reading this. But alongside being open source,

they have also documented the security and privacy side to their service very well on their website; a serious bonus to future customers looking to get secure cloud storage.

Because I haven't used SpiderOak before, I can't comment on the usability or behind the scenes working of the service, so I am stuck going through reviews, reading the content on their website, and making my decisions from a very narrow scope of information. That being said, https://spideroak.com/about/law-enforcement has a line of drool running from my mouth and down my chin. I love it when companies post Law Enforcement Guidelines (Wickr was the first company I noticed doing this). It solidifies their commitment to their users and strives to show the public how much they care about security and privacy online.

The one thing that Tresorit made note of on their website is that SpiderOak doesn't provide you with a way to securely share files in a form such that they remain encrypted from the time they are shared to the time they are downloaded. I cannot vouch for this claim as I have not tried out SpiderOak, but I can say that I am happy with the service that Tresorit is providing. I would only consider switching if it became known that they had implemented a backdoor in their software or if my threat model changed to that where only using open source software was a necessity.

Securing Online Accounts

Hopefully by now you have registered for a ProtonMail or Tutanota account and are ready to start transferring some accounts over. So it is time to discuss some tips for keeping your accounts locked up tight so an adversary doesn't jack them. This section really only applies to non-government entities attacking you for malicious intent. If a Government body like the FBI wants in, a warrant is all they need.

The most important thing to consider is how your account is verified. Most Internet sites use Email because it has been around for so long. So linking up your ProtonMail account makes things all that more secure because your ProtonMail email is incredibly secure from jacking unless someone watches you type both passwords in (which is thwarted by using the LastPass extension in your browser), or you get a keylogger on your computer (which will still likely be thwarted by the LastPass Extention). Even if your ProtonMail account is discoverable to a good portion of the public, because you have either given it out or posted it publicly somewhere like your blog, they still need inside of it to do a password reset on your account.

Next, you are going to make sure you go through the security settings the website provides you with and do some researching on the added security those options provide. Take Twitter for example, they allow you to require Personal Information to reset your account. This means an adversary has to type in your email or phone number to even begin the reset process for your password. Another example would be PayPal requiring you to input your credit card information AND receive an email or text message with a reset code before allowing a password change. But where applicable, always use Two-Factor Authentication.

Two-Step and Two-Factor Verification/Authentication

There is big discussion over whether there are differences between Two-Step Verification and Two-Factor Authentication. It seems like Google, Apple, and Microsoft seem to use the first of the two where most other sites use Two-Factor Authentication (2FA). The idea in separating the two is that 2FA is something physical that you have like a Yubikey, Smartcard, Fingerprint, or CryptoKey. Two-Step Verification requires a second form of authentication alongside your password like a TOTP (Time-based One-time Password Algorithm) code from an authenticator app or a text message sent to your phone.

I shouldn't… but I do use the above two pretty interchangeably. I think the term I use most often is Two-Factor Authentication (2FA) and there is a very good possibility that I am wrong in using that terminology to define methods like SMS-Auth and TOTP but I am going to use it for the remainder of this paper. Generally getting a verification code sent to your email would be considered an insecure form of Two-Factor Authentication because if your email is compromised, they have both your 2FA method and the email needed to reset your password. Likewise, SMS or voice based 2FA is also pretty insecure as your phone provider can be "tricked" (http://www.securityweek.com/hackers-tricked-att-network-solutions-employees-tesla-attack) into giving up enough details about your account to forward your texts to another number and with the advancement in technology, some providers also give you the option to read your messages through their online account portal. The best methods of 2FA are properly implemented TOTP, Yubikey, or Biometric authentication.

"Time-based One-time Password Algorithm (TOTP) is an algorithm that computes a one-time password from a shared secret key and the current time" (Wikipedia). Basically, we install an application like Google Authenticator on our phone and link our account with it by generating and inputting the shared secret. This synchronizes with the current time and generates a new 6 digit code every 30 seconds (usually). After inputting their email/username and password to the website, the user must then type in the 6 digit code generated at the current time by the authentication app. This would be using something you know (password) and something you have (TOTP Code) to secure your account. This is my preferred method for securing my online accounts. All TOTP codes are sent to my smart watch and stored securely around my wrist. I don't even need my phone to login most of the time.

I think Yubico gives a better description of how a YubiKey works for 2FA than I could so here is the excerpt from their site:

> "A YubiKey is a small device that you register with a service or site that supports two-factor authentication. Two-factor authentication means that each time you log in, the service will request proof that you have your YubiKey in addition to your regular username and password. Phishing, malware, and other attack methods don't work because they would need both your physical key and your passwords to breach your accounts.
> Two-factor authentication with a YubiKey makes your login secure and keeps your information private. The YubiKey requires nothing more than a simple tap or touch. There are no drivers or special software needed. You can use your YubiKey on multiple computers and mobile devices, and one key supports any number of your accounts. YubiKeys are nearly indestructible — just add it to your keychain along with your house and car keys."

As for Security Questions and Answers, you would be wise to keep them stored inside of your LastPass account so you can keep them away from the obvious. What I mean by this is instead of using your Dog's name (which could be guessed or identified), you could add a symbol to the front or back of your answer ie: %Baxter instead of Baxter. A maximum-security suggestion would be using random characters and storing them so you don't forget them.

For people who are very active and/or famous on social media, or for business people securing important websites that may be handing important customer details, Two-Factor Authentication is an incredibly important thing to be enabling on all websites/services that give you the option. It may be a learning curve, but it will save you in the end against an attack on your identity.

Full Disk Encryption

One of your strongest counters to surveillance, attack, and theft of your devices is making sure the data on them is secure. Really, the only way to do that in this day and age is to make sure they are full disk encrypted. Full Disk Encryption refers to taking a hard drive inside of a device and encrypting it as a whole so that all the files it has are converted into an unreadable form (encrypted) and not accessible without the password to decrypt them. Some devices, like those running iOS, do this by default. Other's like Macbooks and PCs running Linux, need to have these features enabled and setup. To start, I'll dive right into FileVault2, which is the OSX built in Full Disk Encryption because it is what I use on my primary machine.

FileVault2

Native to all versions of Lion and up, FileVault2 is the advancement on the original FileVault that only encrypted the home folder. It uses 128bit AES in XTS mode to encrypt the disk and is highly suggested when setting up a new computer that has Yosemite or higher. Good strategy here on part of Apple to include a dedicated section about it in the Initial Computer Setup when you first setup OSX. When you set up FileVault2 for the first time, it requires you to have a password on the current administrator account and uses a random number generator (with about 320 bits of randomness available after first boot) to create a recovery key. I would recommend not storing this Recovery Key with Apple even though they give you the option to do so; using 3 security questions and answers for recovery authentication of this key. Instead, I would recommend writing it down on a piece of paper temporarily until you can keep it in an encrypted form (7zip password protected archive) in something like your Tresorit Drive. Once you have securely saved this key, burn/shred the paper you originally wrote it down on. Based on some findings in this paper: https://www.cl.cam.ac.uk/~osc22/docs/cl_fv2_presentation_2012.pdf, FileVault2 uses PBKDF2 x SHA256 and 41,000 iterations on the password. This works to prevent bruteforcing the password due to the delay in checking the hashed password with the one stored on the system. There also doesn't appear to be a limit to the password length so one could in theory create one 100 characters long without any issues other than delay before unencrypting. It is unknown, but unlikely, if a backdoor has been implemented by Apple in FileVault2. If you have a Mac, I would highly recommend enabling full disk encryption to keep your files safe.

LUKS

Short for Linux Unified Key Setup, LUKS is the full disk encryption solution used by many Linux/GNU based operating systems. Typically, it uses AES 256-bit encryption in CBC mode with SHA256 for hashing but that can be edited if needed to run other modes like XTS and decreasing the key size of the AES algorithm to 128-bit. Like FileVault2 for OSX, LUKS has no character limit for the passwords/passphrases and I have tested this with a 212-character passphrase consisting of letters, numbers, spaces, and symbols. The iteration count for LUKS is specified by the CPU power of the machine. For slower computers, this may be lower than wanted so it can be specified with the cryptsetup command. The command would be:

cryptsetup luksFormat -i 15000 <target device>

and I would recommend experienced users setting the value at no less than 20,000. For serious individuals, you would be wise to take that count above 70,000 with a passphrase over 40 characters. LUKS is also fully open source that along with its consistent use within Linux distributions makes it a very trusted choice for FDE.

TrueCrypt

TrueCrypt has been widely known and used by individuals in the data security industry for over 10 years since it's creation in 2004. It was however discontinued in May of 2014 with a post on the official sourceforge website with the company stating that it may contain unfixed security issues. However, TrueCrypt is open source and has passed a crypto audit (https://opencryptoaudit.org/) finding no serious issues with the clean 7.1a version that would compromise the integrity or security of the program.

TrueCrypt provides both full disk and container encryption with varying degrees of security based on chosen encryption algorithms, hashing algorithms, password strength, and more. It has also sadly remained the choice for criminals due to its high level of security and has thwarted government and police agencies from accessing potentially illegal data from drives. The three encryption algorithms that TrueCrypt uses are all 256-bits in size and in my personally preferred order of security would be:

- Serpent
- AES
- TwoFish

It also uses 3 Hash Algorithms:

- SHA-256
- Whirlpool
- RIPMD-160

However, the one issue with the security of TrueCrypt is that although it allows for 64 character passphrases, which are incredibly secure even by today's standards, it only uses 1000 iterations on the password which definitely isn't a big feature for stopping bruteforce attacks. Because of this, it is recommended that individuals encrypting with TrueCrypt do so with a password over 30 characters that includes numbers, symbols, and spaces alongside their words. A good password for someone looking for maximum security but also easy memorization could be:

###33=Pasta..*Jupiter:Drops*fromnoodlesoup======1###

This passphrase is 52 characters in length, memorable by writing it out 60 or so times, but not random enough for you to forget if you don't decrypt your container/drive for a few weeks. It is up to you as the user though to determine what a good enough passphrase is for your level of security. If you are an Edward Snowden reading this, I recommend 60-64 characters and making use of more spaces. Maybe consider using diceware (http://world.std.com/~reinhold/diceware.html) with some added symbols and numbers like:

Hipster…? fluently get argued [+] DIVORSE**660033 american's

TrueCrypt also has the ability to add keyfiles to your container or FDE that act as a second form of authentication before decrypting. Basically these tag alongside your password as something you have and not just something you know. Keyfiles are harder to compromise because they can be stored on a piece of removal media and hidden safely. If you have major concerns about certain files, you could also consider encrypting the media that said keyfiles are on with TrueCrypt and a shorter password while also adding 200+ pictures into the mix. It would mean not only bruteforcing your password, but picking out which 2-3 keyfiles were the correct ones from 200+ pictures on said encrypted media. Pretty secure from my point of view.

VeraCrypt

When TrueCrypt died back in 2014, there was a lot of talk about the security issues that the developers could have been talking about on their website. Was there really security issues? Were they served a National Security Letter mandating a backdoor in an update version be released? Nobody really knew anything above and beyond speculation and it had many people becoming weary. For Mounir Idrassi, that meant taking all of the security issues present in the TC 7.1a release and fixing them in a fork of the project called VeraCrypt. It is considered to be the official upgrade to TrueCrypt by many but lacks the trust TrueCrypt has because even though it is Open Source, it has not yet undergone a cryptographic code audit. I am a firm believer in VeraCrypt as it boasts some serious enhancements to the general security of TrueCrypt while also adding in features of its own that really make the program that much more secure to use.

For starters, they got rid of RIPMD-160 due to it only being 160 bits on the hash and replaced it with SHA-512, which is of course the successor of SHA-256. They also upped the default iteration count in the initial releases to 500,000 iterations on the password, which is a serious, serious improvement over the 1000 that TrueCrypt offered. Recently, they have implemented a feature called a PIM value which stands for Personal Iterations Multiplier and not only gives us a third step of verification to decrypt alongside your passphrase and keyfiles, but also allows us to specify our iteration count in a unique but secure way. When specifying a PIM value for system encryption (FDE), you take your PIM value and multiply it by 2048. For container-based encryption you take 15000 and add it onto your PIM value times 1000. This means you could specify a PIM of 999 and have an iteration count over a million for an encrypted container. Some serious security for your files to be resting inside of.

VeraCrypt has also made some graphical improvements over TrueCrypt, is being consistently updated, and included little tweeks to improve usability, like adding a randomness meter to the "move your mouse screen" to display the random entropy you are acquiring. This to me screams good development and I am hoping for a code audit soon so VeraCrypt can gain the proper attention it needs and we can finally push TrueCrypt into the coffin to be buried. 12 years is long enough, time for the better of the two to finally shine in the spotlight.

iOS Devices

Apple Mobile Devices running anything above version 8.0 are protected with Full-Device Encryption by default known as "Data Protection" in your Passcode settings. However, there is a big leap up from the 5C to the 5S and all devices from here on out that have TouchID. As a starting point, you should refresh yourself on the recent events that have unfolded between Aple and the FBI. I have posted links about this further down in the paper but it should be easy enough to search online. Here is the basics to the encryption your iPhone is going to provide you with if you are running the latest iOS version and either a 5S, 6, 6S, or iPhone SE (and all included +plus+ models as well). If you have one of the listed devices, you will have the best encryption Apple currently offers for their devices. Your iPhone will have a hardware chip inside called a Secure Enclave that manages all encryption and the delays in between password attempts. All versions of iOS above 8 employ 256-bit AES full-device encryption in a unique way that protects all data past the lock screen. This data on the above listed devices is secured using an ephemeral key generated on boot that is entangled with your devices unique UUID to do the encryption. Your passcode protects this key. By default, a 4 digit numeric code is suggested when setting up a passcode/TouchID but users have the option to enable much longer, alphanumeric passcodes for greater security. This is something I would recommend doing.

As well, your device makes use of PBKDF2, as described above, with an iteration count high enough to generate an 80ms delay on passcode inputs (key stretching). This along with a few other security features effectively prevents bruteforce attacks on a device with a passcode longer than 11 characters. The other security features include a lockout after 5 failed passcode attempts and each attempt after that, a Data Wipe feature than can be enabled to wipe your device after 10 failed attempts, and mandating your passcode to be inputted instead of using TouchID when you turn off your device or if you have not bypassed the lock screen in 48hrs.

Alongside the device level encryption that is deemed to be very secure (but not 100% yet), Apple pushed out properly encrypted iCloud backups in 9.3 that use the device's passcode to encrypt the backup. Prior to this, Apple was able to give out iCloud backups when presented with a warrant and a user really couldn't be deemed completely secure unless they disabled these backups on the device. But now, all of your information is backed up securely to iCloud and you still have the option to encrypt full backups to your computer. This being said, I would caution users to not backup applications that store sensitive information to iCloud. You have 2 modes of encryption protecting your device backups to iTunes if you are using full-disk encryption on your computer, but only one line of defense with iCloud.

Recommended Encryption Setup

For an individual who is battling a government level adversary (like a whistleblower), I would recommend the following strategy for keeping very sensitive or classified files from being disclosed to an unwanted third party. Keep in mind that I have never been in such a position so these are just the thoughts from inside my head and may not be entirely well versed with experience. Your first step is going to make sure that your system is full disk encrypted using one of the above 4 programs/solutions. I would recommend LUKS or TrueCrypt with a 50+-character passphrase because they have been well trusted and proven in the courts for many years now (http://scienceblogs.de/klausis-krypto-kolumne/when-encryption-baffles-the-police-a-collection-of-cases/). Secondly, I would have an external drive that was full disk encrypted with VeraCrypt, a 60-character passphrase, and a PIM Value over 800. This will give you an iteration count of over 1.6 million. It is also recommended that you add no less than 2 keyfiles to this encrypted drive and store them in a folder among 200-300 other pictures somewhere on your computer. The encryption algorithm that I would use for this drive would be Serpent(AES) because it relies on two different algorithms that are very well trusted. The hash, not that it really matters, would be SHA-256/512. Once this external device has been fully encrypted, I would then use TrueCrypt to created an encrypted volume on the drive using similar standards but no PIM value (not supported) and no keyfiles (not worth the time). The encryption algorithm would be simple AES to keep the read/write speeds higher. For this container, even a 40-character password with words, numbers, symbols, and possibly spaces is going to be secure enough because it is acting as the internal level of defense. If for some reason there is a backdoor in VeraCrypt, they will still have to get through your TC container's security before getting any of the encrypted files.

Firefox / Tor Browser Bundle Add-ons & Preferences

Generally speaking, plain Firefox is secure enough for everyday people. However, website still do their best to track your browsing habits, feed you advertisements, reduce your browsers security, and even send out malicious content. But there are some really good add-ons you can get for Firefox based browsers that work to proactively increase your security and privacy online. Here are my recommendations for must have add-ons and preferences/settings you should be modifying.

AdBlock Ultimate

This is a pretty big no-brainer. AdBlock Ultimate means no more ads. And for the average person, this will keep you safe from clicking on things that could download files without your knowledge, or attempt to steal your login information via phishing. The only drawback for me is that it removes YouTube advertisements, which ultimately takes away from the potential income a YouTuber would be making. Nonetheless, security and privacy is definitely more important.

HTTPS Everywhere

To help make sure you are always connecting over a secure connection when browsing different websites, HTTPS Everywhere tries all connection attempts to new sites over SSL.

Because a lot of sites don't force SSL connections server side, add-ons like this are a real big boost in security.

NoScript
For people really concerned about their privacy, security, and even anonymity, NoScript is definitely something you should look into. It comes standard with the Tor Browser Bundle (TBB) and disables things like JavaScript, Microsoft Silverlight, Flash, and other plugins that can compromise your browser and leak information about you and your browsing habits. My recommendation is that if you are looking to gain a high level of anonymity online, you always disable Javascript, Flash, Silverlight, and Audio/Video. It disables the plugins you specify by default when you visit a new site but gives you the option to temporarily/permanently enable them for on a site-to-site basis from your menu bar.

Privacy Badger
The Electronic Frontier Foundation (EFF) developed an add-on to help protect you against sites looking at tracking your browsing habits, and spying on you through advertisements that AdBlock may not have blocked. I have it installed but I haven't yet touched it, played with settings, or received any notifications/pop-ups from it. Super nice to know it is protecting me in the background without any effort on my part.

Random Agent Spoofer
One of my favourite add-ons to date is Random Agent Spoofer. It gives you options to change your browser profile and spoof headers to display "falsified" information. You could change your browser from telling websites it is Firefox on Windows 10, to Safari on iOS. One could also spoof the IP address the headers are giving to the websites. I would caution you to be careful with this feature though as in many jurisdictions, spoofing your IP to someone else's may be illegal, especially if you are changing it to one from a federal or state/provincial authority.

DownThemAll!
This add-on isn't really one that benefits you by increasing security, privacy, or anonymity but merely allows you to download large files without interruption. This could be beneficial when downloading a large program or video and your connection is slow. Downloading through your browser may cause it to time out, but with DTA, you don't have this issue. Another good addition to this is being able to verify the Checksum (Hash) for the file via an MDF, SHA-1, SHA-256, SHA-384, or SHA-512 value. This means you can confirm that the file you are downloading is the file you have requested and there isn't a "man-in-the-middle" replacing the file with a malicious one.

LastPass Extention
If you have taken my advice and chosen to go with LastPass to manage all your accounts and passwords, they have an extension for Firefox that I recommend installing. It will automatically input your login details for websites, give you the option to auto-fill forms, and ask to remember password for new sites upon registration. Very easy to use but also really useful.

Firefox Preferences
All browsers come with preferences that you can change and modify to increase or decrease the security and privacy that you will have online. Firefox is no different. I would make the recommendation that all users enable private browsing which will not remember history, store cookies, or keep other temporary files. This helps to both keep unwanted junk off your computer, and disable tracking of your online activities.

For those looking for serious levels of security, privacy, and anonymity, you should type "about:config" into your URL bar and change some of the following settings.

- Javascript.enabled → False
- network.http.sendRefererHeader → False
- browser.safebrowsing.enabled → False
- browser.safebrowsing.malware.enabled → False
- datareporting.healthreport.uploadEnabled → False
- network.dns.disablePrefetch → True

You can read more about what disabling each of these settings does by heading over to the following links: https://www.bestvpn.com/blog/8499/make-firefox-secure-using-aboutconfig/ and https://vikingvpn.com/cybersecurity-wiki/browser-security/guide-hardening-mozilla-firefox-for-privacy-and-security

Virtual Private Networks (VPNs)
There are very few locations where I actually trust connecting directly to the Internet. I don't even do things like online banking or logging into my LastPass from work because the connection is open (not secured with a password/encryption) and thus not secure. My home connection is likely the most secure because it is something that I have personally setup and am able to monitor, but even then, the modem that our ISP supplies that doubles as our WiFi Router doesn't provide the best possible security.

This is where Virtual Private Networks come into play. If chosen and setup correctly, they ensure us a secure, private, and often anonymous connection to the open Internet. Meaning we can browse freely without restrictions and free from surveillance. For the most part, those reading this won't have any serious reason to avoid surveillance, but people have a right to privacy and shouldn't be snooped on. Even if it is just by the sysadmin for the free WiFi at Starbucks. The issue comes down to picking a VPN that suites your needs. Some offer lots of locations globally, others a really great rate and awesome prices annually. I tend to root for and use the providers that offer the best privacy, security, and anonymity, even if it means paying a little bit more. Often times, the cheaper providers are only able to provide such great prices because they pack their servers and don't "really" concern themselves with being all too private. So lets take a look from the perspective of someone who needs top notch security, spyproof privacy, and a high level of anonymity by going through some of the providers I have researched to be the best in these areas. Ideally, we are going to want a provider that isn't based in one of the "5 Eyes Countries" (https://www.privacyinternational.org/node/51) This means it cannot be based out of Canada, The United States, The United Kingdom, Australia, or New Zealand due to their agreement to share information with one another without much

question. They tend to have intelligence agencies (Like the NSA and GCHQ) that do a fair amount of data mining and surveillance on the individuals within their country for “matters of national security”. I would also caution you to stay away from anything listed inside of the “14 Eyes Countries” if you were relying on this provider for your personal safety. The provider you chose should also NOT provide the option for a dedicated IP address. Shared-IPs are strictly the way to go if you want maximum anonymity because it doesn’t single out your incoming IP and matching it with the VPNs outgoing IP. Harder to log/trace, but definitely not impossible.

Accepted payment methods are also a consideration you need to not take lightly. You obviously wouldn’t want to pay with your PayPal or Credit Card if you were looking for full-scale anonymity and personal security. Well-mixed bitcoin that doesn’t link back to you, cash in mail, and PaySafeCards are all methods of payment that are considered to very anonymous if done correctly. Encryption and protocols offered by the VPN Company should also be considered before making a purchase. You will often see the term “Military Grade Encryption” when you are out shopping for a good provider. Generally this just means they employ AES-256 and 4096 bit RSA keys but checking to see if they offer Perfect Forward Secrecy and good Curves for ECHDE Keys is important (http://vincent.bernat.im/en/blog/2011-ssl-perfect-forward-secrecy.html , https://www.perfectforwardsecrecy.com/ , https://safecurves.cr.yp.to/) .

Diving a little deeper into the providers as you shop around, you should check out the server locations they offer and see if they are in jurisdictions that you are happy to be connecting to. This would be a good time to see if any of the sites you want to connect to only work in certain countries (like Hulu, Pandaora, Netflix, etc). As well, like I mentioned above with SSL certificates and how you can check to make sure the site is implementing strong standards for HTTPS, you should be checking the VPN providers site to see what kind of SSL they are using. If they don’t get a grade of A, I would caution against using them as a provider because it shows that they clearly either can't take the time to get a good SSL score (if even just for the promotion) or that they aren’t knowledgeable enough to attain it; a fact that could point towards their service being held up by mountains of false claims. It is also good to see what kind of protocols they are promoting and not just what they are supporting. Most of the good providers will at least ship out a client for Windows and have added features like killswitches and firewalls to stop DNS/IP leaks. However, there are a few providers that I saw who were saying that connecting over L2TP was the best option when it definitely is not. To read more about the different protocols, you can see this link https://www.ivpn.net/pptp-vs-l2tp-vs-openvpn

Below are reviews of the 3 VPN Providers that I have used and trust, one that seems to be very reputable and well designed with good intentions and motives, and the final is one I have used but would NOT trust. You can also check out this link to a Google Doc that was created by ThatOnePrivacyGuy. It documents a lot more providers than just these 3 but is something that has backed my decisions to promote these companies. See: https://secure.link/btlM2Ve1 (See References/Links page at end of the paper for a description of Windscribe’s secure.link service or just type ThatOnePrivacyGuy into any major search engine).

IVPN

To kick the personal reviews off, I have decided to go with the VPN provider that I have been using since early 2013. IVPN, originally incorporated in Malta but recently making the move to Gibraltar due to changing privacy laws, is dedicated to your privacy. They offer 12 countries and a total of 19 servers as of April 2016, which is a fairly small network compared to many other providers. However, I am happy with the locations they have chosen. You can see the full list of locations here: https://www.ivpn.net/status. They market themselves on Twitter as "IVPN is an online privacy service and security service" which to me is a step up from all the Military Grade Encryption and Non-Logging talk that goes around in the VPN community all too much. But like with a lot of their writing, could use some better branding; it just sounds weird having service and service 2 words apart. They state very clearly in their privacy policy (https://www.ivpn.net/privacy) the information that is and isn't logged. The nice thing about connections to IVPN servers is their multihop technology, which allows you to connect through two separate IVPN servers before hitting the open Internet. This gives you as a user more anonymity, as both servers would need to be compromised to compromise your identity, unless they turned on logging of course. Their administration team also informed me that all the VPN servers are running from RAM so everything written is only temporary before being wiped. As a user, I cannot confirm this – but I do trust their word. Hopefully that isn't a misplaced trust.

The encryption protocols used are openly outlined in their "18 Questions to ask your VPN Service Provider" answers on their Support Page (https://secure.link/IgB0DepC). However, they do not give as many details as I personally would have liked. They state that they use AES-256 with 4096 bit RSA keys across the board but fail to mention whether or not DHE is used with OpenVPN. Upon looking through their OpenVPN files given to the user to download, I was able to determine that they are using TLS-DHE-RSA-WITH-AES-256-CBC-SHA:TLS-DHE-DSS-WITH-AES-256-CBC-SHA:TLS-RSA-WITH-AES-256-CBC-SHA for as the TLS cipher suite so you can rest assured that Perfect Forward Secrecy DOES exist on IVPN. They are using the highest level of encryption currently possible for OpenVPN (apart from allowing DSS and SHA1 for older clients haha) so that is a very good thing. You can confirm the encryption used yourself by downloading the .ovpn files from their website and opening them in a text editor.

As for payment and pricing, IVPN is definitely on the higher end at $100 USD for an annual subscription. But they do offer PayPal, Bitcoin, and cash in mail so two possibly anonymous methods of payment are provided and one very easy and renewing method (PayPal). Their plans give access to all servers which is a nice change from the VPN providers that split up their plans based on a bunch of different factors like speed, server locations, etc. Registering was easy and they didn't ask for anything more than an email, password, and my payment. That meant no identifying information had to be given out. IVPN also provides a warrant canary on a monthly basis as a way to say, "Hey, we haven't received any National Security Letters" and an entire section of their website dedicated to pretty much being 100% anonymous while behind a VPN. I suggest you check it out, I have pulled a lot of my own knowledge from these write-ups: https://www.ivpn.net/privacy-guides

As a final note, I have done a lot of verifying with their administration team over PGP encrypted email (pretty awesome that they kept up fairly lengthy conversations with me in an encrypted form), so I have a lot of personal trust with the company. But me having a lot of personal trust doesn't give you the go ahead to also give them a bunch of your trust. You should do your own research and ask your own questions to make sure they are the company that will suite your needs. I do commend them greatly for the work they are doing, but I do not place all my eggs in one basket. Even though it may seem like I worship them as gods, I have just been really satisfied with their service. Your threat model may very well require a provider that does a whole lot more to keep you secure, private, and anonymous (haven't really found one I liked at said level though).

Mullvad

A much less lengthy review comes in with Mullvad, a VPN provider based strictly out of Sweden but definitely not as comprehensive as IVPN. If you take a look at their website (https://mullvad.net), they provide the important information in way more simple terms than I like; as you can see by this already 28 page paper haha. I used Mullvad during my first few months of IVPN and found that they pulled through on all of their statements on the website.

They are based out of Sweden, but allow you to determine where your IP address will be situated (Netherlands, Germany, Sweden, Canada, or the USA). The issue with this setup is even though the servers are shared, you don't have a chance to change the location or even your IP easily. This could present issues if you make a mistake and leak your VPN IP somewhere you didn't intend on. It doesn't give any ability to compartmentalize different aspects of your online life.

They state very clearly on their FAQS page what methods of encryption are employed:

> "Encryption with 2048-bit RSA certificates, DHE-RSA-AES256-SHA for exchange of OpenVPN key material (OpenVPN does not use the TLS data channel for the IP tunnel) and AES-256-CBC-SHA for the OpenVPN data channel"

However, we don't see 4096-bit RSA being used for certificates, which could be a slight downfall, based on one's threat model. Encryption aside, I did like their privacy policy even though it may be seen by a fair chunk of activists, privacy geeks, and even lawyers as being to minimalistic. In part, this shows their strategy for just not putting up with any bullshit… but it also shows us that in some sense, they just don't care to impress. Could be potentially bad for new customers who want to see them go that extra step. I personally think it is a badass move that demonstrates an ability to just run a good VPN without all the bullshit.

I stopped using Mullvad because they didn't offer me multiple servers to connect to without paying for more accounts. I don't know for certain if that has changed but even if it has, the number of locations is still limiting and I wouldn't want to go back to that. With a provider like IVPN, I could dedicate certain server locations for certain things. One for business, one for anonymous activities, one for personal things while connected to insecure wifi, etc. I can't do that with Mullvad so even though I would rank them very highly in terms of security and privacy, the anonymity aspect falls short and that sucks.

Cryptostorm

Lastly, we come to a provider that I only really started looking into in around September of 2015. I was still very satisfied with IVPN but my subscription was coming to an end, which meant another long process of anonymizing a method of payment and I wanted to make sure that the company I was going to continue to support got the most stars in my personal ratings from my "shopping" online. I had heard some amazing things about the CS Network and wanted to see what they were all about in more in-depth than just browsing through their site like I had previously done a few years back.

The first thing you'll notice when you go to Cryptostorm's website is what many perceive as a mess that is difficult to follow, hard to read, but somewhat appealing. It is unlike any of the other providers and almost unprofessional; but that feeling of difference seems to draw me closer. Sort of like how Mullvad was so straightforward and minimalistic, the odd nature of Cryptostorm's website tells a story of diversity. To start, they are a company that is based out of Iceland but handles all of their financials out of Quebec in Canada. Iceland is a good privacy centered country to be incorporated in (although they don't have a central office anywhere) and I have always liked .is domains.

Navigating through their website was pretty difficult to acquire the information one might want when choosing a provider so I took to their IRC to get some of my questions answered. I was unfamiliar with token-based authentication before asking around and getting a more detailed response but to my knowledge, it replaces user/pass authentication with a generated token that must be hashed before use. This token is random; hashing it makes it even more random. So the server should never have any information about the users at all if they pay using anonymized Bitcoin (which is the preferred payment method that they offer). The encryption that is used is not clearly located on their site so one has to dig slightly deeper and head over to their GitHub to check out the .ovpn config files yourself. This is what is displayed:

```
ns-cert-type server
auth SHA512
cipher AES-256-CBC
replay-window 128 30
tls-cipher TLS-DHE-RSA-WITH-AES-256-CBC-SHA
tls-client
key-method 2
#log devnull.txt
#verb 0
#mute 1
```

The encryption used appears to be very high-grade using DHE for perfect forward secrecy, 256-bit AES, and SHA512. However, this doesn't designate the size of RSA keys being used. After contacting one of the administrators about the encryption used, this was the reply email I received. Really goes to show you the quality that is provided by Cryptostorm when they are willing to go to this degree to provide for their customers. https://cryptoseb.pw/cryptostorm-reply.txt

A current work in development for Cryptostorm that would seriously decrease the risk of correlation attacks or the possibility of your IP ever getting leaked, encryption keys compromised, or identity exposed is known as Voodoo. You can read more about that up and coming idea on the GitHub page for it here: https://github.com/cryptostorm/voodoo.network

As far as a Warrant Canary, Cryptostorm does not offer one and doesn't seem to have any plans to do so. Instead, they offer a "Privacy Seppuku Pledge" which is their way of saying we will shutdown, wipe the servers, delete everything, and play dead before giving up information about our customers. You can read more about that pledge here: https://cryptostorm.org/viewforum.php?f=63

Overall, I am very confident in the service provided by Cryptostorm and certain that an individual, with a moderate threat model, could receive maximum security, privacy, and anonymity from using their VPN. They are like the nerd at the front of the classroom that is incredibly smart, but very hard to relate with and understand. And I think that is a good thing!

OVPN.se

I have never used OVPN.se so this little review will be entirely based on what they "claim" to be doing. However, their claims are definitely a good thing if they don't ever turn out to be lies. For starters, the company is based out of Sweden, which is a 14 eyes country yes, but one with pretty good privacy laws. VPN providers aren't required to keep logs in Sweden so that solves a lot of court orders if the company has good intentions.

Their hardware is slightly different than other providers as they claim on their website that they have completely removed all hard drives, USB sticks, and CD-ROMS from their servers and do everything from a localized "boot server" within the data center. See: https://www.ovpn.se/en/blog/improvement-of-the-physical-security/. This is a big security enhancement for customers because it means one more hoop they would have to hop through to enable logging, as they would have to send all those logs over the network to another server for storage. They also claim to keep absolutely no logs (and they explain it in their blog too), which must be a diagnostic nightmare the second any issues arise. Not all logs are bad logs people.

The company also providers their PGP key for communication (https://keybase.io/ovpn) and have it hosted on Keybase but have neglected to even upload a profile picture let alone verify their Twitter account. Taking the extra time to pay attention to detail like the other providers above have (except maybe Mullvad who is clearly making a statement about detail aha), is going instill better trust in both current and future customers. This trust could be furthered if they provided a Warrant Canary. Something that has been asked around quite a bit over Reddit but still not implemented. As well, they seem to be a company who has big dreams of deploying all this physical security but then use 1024 bit TLS keys for the AES key handshakes alongside 2048 bit RSA keys. There are no performance drawbacks to using 4096 bit keys and even though 2048 bit RSA keys are a ways from being cracked by any Government agency (to my

knowledge at least), it just looks better for your company if you are employing what should be considered the security standard.

Overall, I feel like OVPN.se is doing a lot in terms of protecting our privacy and keeping us anonymous but like anything, they could definitely be doing better. The lack of attention to detail is concerning because it implies that if they aren't taking the time to upload a profile picture, or be actively engaging with their audience at least a few times a week, what else aren't they taking the time to do? And is that affecting the privacy, security, or anonymity of the user-base? If I had to 1 out of 10 rate them, they would be midrange at about a 7.

Private Internet Access (PIA)
I used to be a user of Private Internet Access as a VPN Provider, but the key words there are "used to". I will never go back to that company even if they completely remodel everything about their service from the ground up. I have posted on a few different forums about why but I will give you the gist of things here.

1) Individuals need to be certain that the company they are entrusting with their life (in some cases), is going to protect them when @#%$ hits the fan. This is not the case with PIA
2) Their homepage depicts a family riding on their bicycles. Uhmmm… since when did this have anything to do with Internet Security, Privacy, and Anonymity?
3) Their contact page depicts a typical support agent wearing a headset but they make no mention of being able to call their support. So why is she wearing a headset used for voice communications
4) They have only recently outlined their encryption protocols. In the past, you had to message their staff to get details, and the response was nothing great.
5) When I asked their staff around a year ago if they had a PGP Key for secure email communications, the response was "PGP is not an encryption method we offer [pasted text about the encryption they offer]". Too bad I didn't screenshot it for proof!
6) They seem to state with several infographics on their website that ANY information you send over the Internet is going to be unencrypted without Private Internet Access and claim that with their service, you are automatically anonymous as well. Re-read the last.. I don't know 26 pages of this paper if you believe them. VPN does not = anonymity and not using a VPN does not = insecure
7) They have had instances in the past where they have clearly handed over customer information even though they claim they can't do so based on the design of their VPN service. See: https://secure.link/2jBqOcMU
8) Their Twitter handle is literally "buyvpnservice". Do I need to go into how much of a crock this sounds like to a potential customer looking for good privacy? If you have made it this far in the paper and can understand 90-95% of what has been written, you can hopefully agree.
9) Their Promotional Video makes false claims that using Public WiFi means people can spy on you with the click of a button. Please refer to the section on HTTPS encryption for

browser-website-browser and then point me in the direction of this magical "button" that does this for me.

10) They are incorporated in the United States. See the section on "The 5 Eyes" below.

Firewalling Your Network Connections

One of the other ways one can secure their connection to the Internet is to make sure that all incoming and outgoing connections are being passed through a Firewall. This enables a trust vector in assuring your install applications aren't connecting to or receiving connections from shady looking servers. The program choice is really up to user-preference so the ones listed here may not be ones that you trust, or have heard good things about. Nonetheless, these are the ones I have used before and was done well by.

Windows

I haven't spent an incredible amount of time using Windows while on this security/privacy kick but the time I have spent using it, I was doing my best to make sure my security was top notch. I haven't been in the "Windows Scene" recently but I am still hearing good things about PeerBlock and Comodo Firewall as standalone firewalls for your system. PeerBlock has been out of development for quite a while though so I am skeptical but Comodo is still being actively developed. Personally, I like Kaspersky as an all in one but something with more versatility like Comodo is nice. The idea is to have something installed that will alert you with connection attempts both incoming and outgoing. Windows isn't very secure in and of itself so an all in one antivirus/malware, and firewall like Kaspersky might be your best bet. You would also be wise to install something like Malwarebytes Anti-Exploit (https://www.malwarebytes.org/antiexploit/) to help shield you from exploits that attack things on your system like Java, Flash, PDF Readers, and media players. For top the line Windows security, please see: http://discourse.ubuntu.com/t/how-to-completely-wipe-windows-8-and-install-linux/1416

Mac OSX

Generally, OSX on Mac Systems is a lot more secure than Windows because of the design. Everything is compartmentalized and the sandboxing on OSX is significantly better than Windows. However, right out of the box, a brand new Mac is not as secure from adversaries in 2016 as it generally was in 2010. You need to spend some time to get a very good level of security if you want to be safe online. Especially if you are an individual combatting hackers, government-level adversaries, and the like. For starters, head into your security preferences, turn on OSX's native firewall, enabled stealth mode, and do not allow signed software to automatically accept incoming connections. This will do a really good job of protecting you from the outside in and stopping attacks before they do damage. Then, you need to make sure you are protected from the inside out and buy yourself a license for LittleSnitch. It is without a doubt the best Firewall solution for OSX that deals proactively with outgoing connections. This stops applications you have installed from accessing the Internet without your consent and only on the ports, and duration that you specify. Once you have read some tutorials on how to use it, start playing around with the settings. After a while, you should be able to get some really good profiles working for different environments. I have one specifically designed to block all

connections when I connect to an unknown network. And another that restricts my system to the very basic necessary services for OSX to run then only allows the Tor Browser on top of those. With the addition of my VPN connection, this makes sure that my IP isn't leaked when I am looking for anonymity.

Another good consideration is to install BlockBlock and KnockKnock from objective-see. BlockBlock monitors the persistent locations in OSX and gives you an alert when an application tries to write to one of these locations. This protects you from malware that is trying to keep itself running and active even after reboot (hence the "persistent" terminology). KnockKnock tells you what is already persistently installed on your Mac and gives you a good breakdown with VirusTotal integration to determine if these items are to be considered malicious or not.

Linux/GNU

IPTables is the generic firewall that ships with all distros of Linux to my knowledge but it is a pretty sharp learning curve if you aren't a Linux Guru. If the Linux distribution you are running is going to be on a server without really any graphical interface, CSF is a really good addition that works alongside IPTables nicely. CSF stands for ConfigServer Security & Firewall and comes with both stateful packet inspection and login/intrusion detection. However, if you are going to be using a graphical version of say Debian for your home/work computing, you could consider using a firewall like Zentyal (https://wiki.zentyal.org/wiki/En/3.5/Firewall) or ClearOS (https://www.clearos.com/resources/documentation/clearos/content:en_us:6_custom_firewall). But because on personal computers there isn't a remote connections or anything like SSH running, you don't really have a need for a firewall if you trust the applications you are installing. Here is a good article on whether a firewall is needed for Linux/GNU based operating systems: https://askubuntu.com/questions/344176/do-i-need-a-firewall-for-my-desktop. I have never used one in my days of running Debian, BackBox, and Kali on my laptop.

As you can tell from the above, OSX and many forms of Linux/GNU are more secure out of the box than a Windows install is going to be. Microsoft is getting better, but damn they aren't to the point of not needing protection yet. I would say the best bet for someone needing really good security/privacy/anonymity with their OS would be to install Debian or SubgraphOS (both discussed further later on). I like the look and feel of Debian as a personal computing OS but am still true to OSX for most things because it is what I have used for the last 4 years. But don't get me wrong; there will always be a VM of Debian and Kali available on my desktop!

Government Level Individuals

Another Introduction
First, I want to point out how difficult this section was to title. Going one step higher on the ladder of this Crypto | Paper, you would generally see people like journalists, freedom rights activists, individuals fighting for online privacy, members of government, or larger-scale business executives. That was just way to hard to try and incorporate into a section header so I have chosen to go with "Government Level Individuals" because in one form or another, the people who will benefit the most from this section of the paper are going to be either tied heavily to a government body, opposing one, or straight up under attack from one.

I must also point out that I do not condone illegal activities. However, in saying that, much of this section might give you the vibe that it is tailored to criminals. That isn't the point though. I just want to provide as much information from my own experiences and research as possible and writing about these things in a context like that helps to get it all out in the clearest possible manor.

The "Five Eyes" Countries
To start, let's take a look at this idea you may have heard of called the 5, 9 and 14 eyes countries with a heavy focus on the initial 5, what they are, and how they are working to take our privacy away in nearly every aspect of our life. Well, how certain bodies of Government within these 5 countries are working against our privacy. Not all forms of Government are "bad" per say.

The "5 Eyes" countries refers to 5 countries (The United States, Canada, The United Kingdom, Australia, and New Zealand that have an intelligence agreement known as the UKUSA Agreement (Wikipedia) to share information with one another. Many experts claim it is one of the largest espionage alliances in history. The NSA, short for National Security Agency, is the department of the government in the United States that is responsible for the global monitoring, collecting, and processing of information as it pertains to the United States and its national security. Basically, they mine tons of data and make sure it doesn't scream F#@K the USA. They are responsible for a program known as PRISM, which was founded to allow the NSA to collect data seamlessly from major tech companies like AT&T, Microsoft, Dropbox, and Facebook. Similarly, the United Kingdom has a company known as the GCHQ or Government Communications Headquarters. The GCHQ is a British intelligence and security company tasked with providing Signals Intelligence and information assurance to the British Government. To put it bluntly, they spy on their citizens. Proof is in the pudding with around 5.9 million CCTV cameras in the UK (http://www.wired.co.uk/news/archive/2015-08/17/one-nation-under-cctv). They do very similar duties as the NSA but deemed to be a lot worse and on a much larger scale but both are likely in complete cooperation with each other.

For people looking for a high level of privacy and anonymity, this alliance of "5 Eyes" is incredibly infringing and takes away our personal security entirely. You may often see that one friend always sharing these anti-government, tinfoil hat, big brother is watching us posts on Facebook. The interesting thing is, the government organizations being discussed in these posts exist for that very reason. They may not be watching you precisely, but they definitely have information on you. Information archives that only get bigger with our move into a more technological and digital world. So consider this when you are out exploring your options for different services to fit your wants and needs online and be sure to take a peek at where they are incorporated and whose laws they have to follow. Don't be fooled into thinking that because the US has some great constitutional rights belonging to each citizen that there aren't loopholes. If a senator says one to many negative things over unencrypted phone calls, word is going to get out about these conversations even if the people they are talking too keep their mouth completely sealed. Surveillance keeps us safe to an extent… but it also removes the privacy we have a right too. See this Reddit post on the 14 eyes for more information: https://www.reddit.com/r/VPN/comments/345nep/psa_avoid_servers_and_vpns_in_the_14eyes_countries/

Breaking Down A Service: *What's Really Under The Rug?*
By now, the hope is that you have really begun to look at the services you are using on a day-to-day basis. Maybe you have run a few SSL tests on the websites you login to, or checked out some privacy policies to see how they handle your information, or even gone so far as to contact them to get some details on the encryption standards they have. Either way, you are beginning to break down the services you use to see what is really under the rug. Another really awesome way to do this is to not go straight to the company but to other sources on the Internet. Typically, and rightfully so, they will be biased towards their own service; especially if it means they could make some money off of you. So those companies might not be completely honest. A little white lie here and there never hurt anyone, right? Wrong! It is hurting you. So go to the companies for the little details, but then take to the Internet for a bigger, broader idea of what is really under the rug. Type, " is [COPMANY/SERVICE HERE] safe" into Google and see what comes up. Here's one as an example: https://www.google.com/search?q=is+bitlocker+safe&ie=utf-8&oe=utf-8. The very first link that shows up when I click that is titled, Can the NSA Break Microsoft's BitLocker?

Not every company you use is going to be 100% when it comes to securing your online identity, keeping your information, data, and communications private, or giving you a full-scale shield of anonymity. But you should still be concerned with the companies that are claiming to do that. Take Wickr and Signal for example. They are prime examples of companies that are very proactive in protecting our right to privacy online, but have some "flaws" that are only really seen when we pull up the rug. For starters, Wickr isn't open source. Which in and of itself is the biggest flaw for the company. You can't verify that they haven't handed out a backdoor to a third party. You can't confirm that the encryption they are using is as strong as they claim it to be. And you can't vouch for their motives on the same level as a company like Open Whisper Systems who runs/develops Signal. But on the other hand, Signal isn't this miracle product either. It jumps through hoops and climbs mountains to keep our communications secure and

private, has one hell of an encryption backbone, AND is committed to an open-source company model. However, through all this privacy and security the anonymity we need is lost the second we have to input our phone number and use it as a method of other people to contact us securely. That means I would have to post my cell phone number in a public form like on my website or Twitter Bio for someone to hit me up on Signal. This isn't happening, ever. My Cell phone number isn't something that should be public knowledge. If it were to be public knowledge, my online identity and personal security becomes shot.

By Design, By Choice, or Both

Once you start to break down the companies you use or the ones you are looking at using in the future, you should start to get this idea of which companies are building their products to be secure, private, and anonymous by design, which companies are building them to be secure, private, and anonymous but on their choice to not disclose information, and which ones are doing both. Wickr would be a company that is doing it by choice, as they seem to be completely dedicated to sticking up for our right to privacy but can't prove it 100% because they lack an open-source product. ProtonMail would be a company that is doing both. They have designed a service that is secure by design and are choosing to hold up values and beliefs that protect our privacy in the digital world.

Ideally, choosing products & services that are doing both is the way to go. The people behind the scenes need to be making products now that are secure by design. I like the term that was used in the recent struggle between the FBI & Apple over the San Bernadino's Phone (Read more here: https://www.apple.com/customer-letter/ here: http://www.zdziarski.com/blog/?p=5645 and here: https://secure.link/xityuzF1). I can't say for certain whom it was, but on my Twitter Feed, the term "Warrant Proof" surfaced and geez do I love it. The basis behind the terminology is that a company develops something that even a warrant isn't going to break. Which is really awesome because it both shows the commitment on the company to build a device that even they can't get into, and their devotion to holding up good principles that strive to protect their customers and users.

Coffee Break

Time for a little bit of a coffee break where I state again that I in no way condone illegal activities but continually feel like I am advocating for criminals as I type. But to me there is a difference between abiding by the law (which companies need to be doing without a doubt) and fighting against Governments that have done everything in their power to relinquish the privacy and security we have online. If you even talk about opposing the government in many countries, you can be labeled as an extremist and sent to death row. How is that fair? Now, this doesn't hold true for the majority of the first world countries we live in today, but we still have bills being passed that strip us of our rights. This video by Mozilla does the best to explain the reason I stand up for strong encryption and companies that advocate for our privacy: https://advocacy.mozilla.org/encrypt/social/1. I already have a hard time explaining certain things to even my family like topics regarding personal health matters, relationships, and such. It pains me to think of a world where some random member of my government, or even

another government could see this information. I want to be able to share information with the people I designate, not anyone who happens to be looking my way.

FOSS

Getting back to the good stuff, I have talked in the above pages about a term called FOSS or open source, or the long form Free, Open Source Software. This refers to a program that has its source code published in a free manor (ie without restrictions, not pertaining to money), for the public to look at. The preferred way of opening the source code of a program, service, or application is to submit it to a website like GitHub, SourceForge, or Bitbucket and allow the public to view it. When it is published to these sites, it is also easy to track changes to the code as the developers publish new versions. You can then in some cases, if they have developed the program for your operating system, build the program from source yourself. This would give an expert the ability to inspect the code, determine whether or not it is legitimate like the company states, download it, and compile the program from it. This individual would thus be getting the most out of the service and maximizing their security model. The one issue that has arisen with Open Source Software however is the fact that many of these applications are being downloaded onto Smart Phones without reproducible builds. This means once they have hit the App store (iPhone) or Play Store (Android), we can't confirm whether the application we are downloading is the same one being showcased in the source code they have published. For the most part, this shouldn't be deemed a concern. However, let's say you are communicating some really sensitive and potentially illegal information through an application that is Open-Source and thus garnered your complete trust but the company behind the app is pushing out a false app to the App Store. You would be communicating through a backdoored version that is logging everything and handing it to the police. This is a very unlikely thing to be happening, but hey, Edward Snowden isn't/wasn't the only person fighting for his life in the digital world.

G/PGP Based Encryption & Authentication

One of the other things you will have likely noticed me touching on is companies who are willing to share their PGP Key for customers so they can use email + PGP for communication to support. First, let's tackle the difference between PGP and GPG. PGP is short for Pretty Good Privacy and was developed by Phil Zimmerman in 1991. GPG is short for Gnu Privacy Guard, which is an adapted version of this released in 1999. And OpenPGP is the standard that both pieces of software are compliant. So when people talk about GPG keys, they are technically still PGP keys but ones that are derived from a GPG program like GPG Keychain for OSX. On my website, I have listed my key as G/PGP because it is a PGP Key using the GPG software.

Typically PGP keys are used for both communicating securely in an encrypted form, and signing messages that can be validated for authenticity. G/PGP is the basics of generating a private key and a public key to a user. These keys could be compared to 2 pieces of a puzzle that are each the size of a football field, containing hundred of thousands of little notches along each side. The public and private keys that are generated are the only 2 puzzle pieces that will fit with each other. Once generated, one distributes their public key and sends it to key-servers on the Internet that store it for retrieval by others. However your private key, which is protected by a long passphrase, is kept private and should never be distributed publicly. Once your public key

has been distributed, people can use it to encrypt messages to you that can only be decrypted by your private key. You could also sign a message that would protect it from being altered. Users could then take the message and use your public key to validate the authenticity of the message. If even so much as a space was removed, the message would not verify correctly and the recipients or audience of the message would know it has been altered. This is especially useful in security related messages from a company/website like signing notifications and updates to verify that the website owner is the one posting said messages and not a hacker or Government body.

Recently, I purchased ProtonMail Plus, which meant linking up my domain name with ProtonMail so root@cryptoseb.pw was routed through their servers. This however meant that the email I added to my primary PGP key was not the email I was giving out to the public. Same inbox, different email. Check out my method for switching over to a new key with my new email while still maximizing the trust vector for those who communicated frequently with me or simply had my old PGP key saved: https://cryptoseb.pw/new-key.txt I'm not saying this is something everyone would need to do. However, I wanted to make sure the transition to a new key couldn't in any way, shape, or form be misinterpreted as malicious or my security being compromised.

If you are an individual inside of this category, I would say it is prudent that the generation of this key is done on a system that has networking disabled with your GPG program of choice firewalled to block all connections to and from keyservers. The last thing you need is a backdoored program maliciously uploading your private key somewhere without your knowledge. Yes, your private key should have a very strong password protecting it from attacks like this, but it also shouldn't be "that easy" to steal. Your GPG program doesn't need to do key retrieval or anything like that as importing them is simple with copy/paste so no point in letting it access the Internet at all.

Warrant Canaries & Signing Messages

Service/Websites owner and companies can and should be publishing a Warrant Canary to the public at least 4 times a year. The definition from Canary Watch (https://canarywatch.org/) reads: "Warrant Canary is a colloquial term for a regularly published statement that a service provider has not received legal process that it would be prohibited from saying it had received, such as a national security letter. Canarywatch tracks and documents these statements". Many major websites post Warrant Canaries in an attempt to protect the people using their service. These can be viewed on the website linked above. A good portion of the companies posting Warrant Canaries are using a PGP key that they have made public to sign them. This allows them to provide a sense of trust that the message they are posting has not and cannot be altered without completely re-signing a new message. A good example of a signed canary in this form can be viewed on SpiderOaks website: https://spideroak.com/canary. This form of Canary is rather difficult to make sense of, but provides a very advanced level of security for their user base. Basically, they have decided to sign each Canary with 3 different keys that have been distributed among 3 different administrative individuals from around the globe. These 3 people are supposedly not in the same countries/jurisdictions with one another so to compromise the

validity of the Canary, law enforcement would not need to force 3 users to give up their private keys and passphrase, instead of just one body or individual. Another nice addition to this canary over all the others I have seen is how they have included all previous canaries when posting the updated version. The only issue with posting a canary like this is that it is difficult to validate. They post instructions on their website (https://spideroak.com/articles/on-status-reports-transparency-and-overall-safety) but even so, it is a time consuming process that even I had a hard time understanding. Definitely not for the average user.

Another nice addition to the Warrant Canary is validating that the message has not been previously created. IVPN (https://www.ivpn.net/resources/canary.txt) does this by adding in headlines and corresponding URL links from a big-name news website on the date that the canary was posted. This confirms that they hadn't pre-signed a message saying all is good, kept it on one of their systems, been compromised by a body of law enforcement, and then posted falsely.

My biggest concern with the traditional Warrant Canary is that it is flawed in a sense to me. Unless you are going to sign the same message like 3 times over by 3 different people from 3 different countries globally, you really can't be certain that the signed message is legitimate. My reasoning behind this is that although it has been debated on whether or not a company can be compelled to "say something", we can't be certain that they wouldn't say something if they were asked. I am referring to the idea that a company like IVPN can't be forced to write a falsified message and sign it… but how do we know they haven't been doing that all along? How do we know they haven't already been approached a year ago and just been lying to us this entire time? It is a rocky road and I don't think we have found the best solution yet.

Gaining Some Serious Anonymity

The above 35 some pages have been focused around security and privacy but have only dabbled in the field of anonymity. But for "Government Level Individuals", anonymity is no joke. Especially if you are an individual who has the potential to become a target for government level adversaries. Take into account when reading this next little bit that we may have touched on some of these topics above. I am however going to try and go into a little more in-depth here.

The Tor Network & The Tor Browser Bundle

My first step in looking at anonymity is making use of the TBB and the Tor network. Tor was released in 2002 and has since evolved into a tool that is used by millions of people worldwide. Tor enables users to browser the internet, chat with other people, and access "hidden sites" (websites with .onion appended to the end of them that generally cannot be viewed in a normal browser over regular internet). The Tor network is used by freedom rights activists, privacy advocates like myself, whistleblowers, journalists, and even criminals doing illegal things like selling drugs and distributing child porn. Because of that last little bit, I dislike the fact that Tor shields individuals so well from being caught, but I also feel that it is a great tool for protecting your privacy in a world where we are constantly being monitored and watched. It's a hard boat to be in when on one side of the river, you have people literally fighting for their right

to freedoms and free speech, but only the other side of the river, you have people doing ridiculously illegal things.

To understand how Tor works, you first should see this picture published by the EFF: https://thenextweb.com/wp-content/blogs.dir/1/files/2013/10/tor-workflow.jpg. Basically you are connecting to a network that is routed through three separate servers from around the world before sending out data from your computer to a website and then returning data from said site back to your system. These servers are referred to as "nodes" and make sure that your data is fully encrypted while in transit to the destination site. If the site you are connecting to over Tor does not make use of HTTPS (SSL Certificate for encryption), then the connection between the last node (Exit Node) to the website's server will not be encrypted but you will still be anonymous to the site. The encryption that happens is done at the packet level see: https://i.stack.imgur.com/RSRkz.png, which means information isn't viewable even if it is intercepted in the middle. There are a few known attacks on .onion sites but many of them fall into the category of failing to correctly setup the server hosting the site. A prime example of this would be with a hidden service known as doxbin. The server it was hosted on was seized after 3 months of denial of service attacks to pinpoint its location. For more information on the different attacks against Tor Hidden Services, see: https://www.google.com/search?q=.onion+attacks&ie=utf-8&oe=utf-8. Google, and likely your Internet Service Provider are likely monitoring search results. It would be interesting to know just what this logging looks like. Alternatively, you can type "Attacks on Tor" or ".onion attacks" into DuckDuckGo. The only attack I know of against Tor users is to exploit plugins they have installed, JavaScript/Flash in the browser, or by profiling them and getting bits and pieces of information about them over time. There could however be zero-day exploits available to Government Bodies that we are unaware of. So using a VPN behind Tor isn't such a bad idea.

To get the most out of Tor, you should refer to the section on Mozilla, the add-ons to install and preferences to change in your about:config. But I would like to CAUTION YOU that installing a bunch of add-ons increases your chances for exploits to affect you and also actively increases your fingerprint. The idea behind using Tor to gain anonymity is to be like everyone else… so just disabling JavaScript/Flash but leaving everything else rather Plain-Jane is likely going to be your best bet. The people behind Tor have developed it to be secure and anonymous with a fresh install so the only thing you really have to do is go over the settings to make use of the built in features.

Keeping Personal Information OUT

If you are reading this but have no need for anonymity and really can't see where it would fit into your Internet life, I at least hope you can imagine a situation where someone else might need it. To maximize the anonymity you can acquire on the Internet, you can't just do things like buy a VPN, use a good email provider, and browse through Tor. You also need to consider the information you are posting on the Internet. A general concept people use to disguise themselves is to post Disinformation (http://www.merriam-webster.com/dictionary/disinformation), or information that is purposefully false/fake. Most of the time, people do this by coming up with an alias or alter identity that consists of a username

that isn't like their other ones and creating fake accounts that don't link back to them. So if I wanted to communicate anonymously with someone and not let them know who I was, I could acquire a VPN account and register for a Tutanota email or Wire account and message them while connected to my VPN and/or the Tor Browser. As long as I didn't give out identifying information about me like my name, location, age, or links to real media, I should be safe from an attack.

To take this one step further, you can attempt to remove all of your other personally identifying information from the Internet. Keep in mind though that this is generally a very hard challenge to overcome because once it is online, you can't be sure it is ever going to get erased. This is why it is important to try and minimize the information you are posting based on the kind of threat model you have. It helps in situations where you need to hold up a persona online but not have said alias connect in any way to your real identity.

Cell Phones = Rarely Anonymous

It isn't so obvious why after we discussed earlier about the strong encryption on a newer iPhone, they might not be considered a tool for anonymity but it is true. Cell phones are not devices that aid in you being anonymous. Take a look at your cell phone from a different angle for a second. It has ties to your Internet service provider, who has the ability to monitor all incoming and outgoing calls and texts that are not encrypted. Furthermore, they aren't usually built to allow a bunch of tailoring to fit your needs. One can't just throw a version of Debian on there without some serious background knowledge. As well, we are getting into a very digitized world where companies want to know our location and they want to be able to track that location to tailor their service to fit your needs. But in having these devices that potentially record our every footstep, we are removing ourselves from the anonymity we so desire. This is why I like services that work on both mobile and desktop environments. They give you the option to have a very usable and ready environment on your mobile device, but also the full frontal secure, privacy, and anonymity a desktop environment can give you.

Metadata is a Killer

Literally, I bet metadata has killed someone before and burned the… nevermind. Metadata is data that describes other data. An example of this would be the email header contained within each email you send. It contains identifying information about the sender, and how the receiver is to read the email. But metadata can be a serious hindrance to your online security. It comes in all forms, and in many instances, you have to really know what you are doing to circumvent it on your own. Say you send a picture to someone that you took of your dog on your iPhone over email. You chose to send this picture through ProtonMail to make sure that it was fully encrypted and your IP address was stripped from the header. One would assume that you are making use of good security and privacy tactics, right? But the truth is that you would be wrong. As I said before, metadata comes in all shapes and sizes and is even located inside that picture of your dog. Your iPhone that was used to take said photo recorded a lot of information about the photograph and stored it along with the image. Things like the data and time it was taken, size of the image, device it was captured on, and even the location where the photo was taken can all be included inside what we call the EXIF data on the image. So simply sending an image

to someone could have completely ruined the work you have done to remain anonymous. Privacy International has more talk about metadata that you check out at this link here: https://www.privacyinternational.org/node/53

Paying For Something "Off The Record"

The issue with anonymity is that it is fairly easy to acquire online until you have to pay for something. This is due to the fact that generally, our government always wants to have tops on our financial situation so it is rarely known to just a very select number of people. However, to acquire this level of anonymity, we typically need to have a VPN account to secure and anonymize our connection to the wide-open web. Purchasing a VPN with our credit card or PayPal account will link back to your personal identity because as I said, the government likes to know what you are up to when it comes to money and big companies like PayPal, instill methods to make sure you aren't creating fake accounts. But many people still need to be able to purchase things "off the record" so that tracking them becomes a lot more difficult. One of the preferred methods of paying for things has been forms of crypto currency like Bitcoin. The one major drawback to purchasing Bitcoin is that the price of it fluctuates on a daily basis so one moment you are making money and the next you are losing it. The positive side to Bitcoin is that you are able to both purchase it with a degree of anonymity (if you can buy with cash) and are able to "mix" your BTC (see: https://bitmixer.io/ and https://en.bitcoin.it/wiki/Mixing_service). There are also a wide variety of services on Tor that allow you to mix your Bitcoin. However, the legitimacy of such services is sketchy at best so use them with caution.

As much as I like Bitcoin, I always have an issue when it comes to mixing it. I am scared the service I am mixing with is just going to take my coin and run away. So because of that, I prefer to pay with cash in mail, or PaySafeCards. I will discuss cash in mail in the next paragraph, as it is a bit longer of a process than using PaySafeCards, which is super easy. The cards can and should be purchased from a retail outlet with cash and then a 16-digit code is scratched off on the back. For services that accept PaySafeCards, all you have to do is input the 16-digit code. No activation, billing information, or confirming anything what so ever. They are really good ways to purchase in private.

With cash in mail, things are a little more complex than simply getting a 16-digit card that you can use for your online purchases and isn't often as widely accepted. However, most VPN providers will allow you to pay with cash, even if they don't already offer it as an option, by simply contacting them and inquiring about using it as a payment method see: https://www.ivpn.net/knowledgebase/91/How-can-I-pay-with-cash.html
IVPN also offers a tutorial on how to pay anonymously with Cash and Bitcoin (which by the way only furthers the trust I have for them) that can be read here: https://www.ivpn.net/privacy-guides/advanced-privacy-and-anonymity-part-7. The only thing you really need to consider is that an ATM may very well record the serial number from the cash and link it to your account that you just withdrew it from. So go ahead and take out $60 or whatever to pay for annual subscription to your VPN account, but then go down to your local market and ask them if they can exchange it for different size bills; like say a 50 and a 10. You also run the risk of someone

opening up the letter or package in which you are sending the cash and stealing it. This means you are out the money but still need to pay for your product/service.

Destroying What Is No Longer Needed

After you have put all of the above pages to good use, you are going to be left with a lot of unneeded data. This data could include cache information, temporary files, browser history, chat conversations, and even records of your transactions. These are all things that can compromise your security if you leave them sitting dormant. Plus, they really don't serve any great purpose other than to keep track of your history so getting rid of them is pretty beneficial. To begin, you need to identify what information is being stored and where. A good way to do this is by going through your computer top to bottom and checking through typical folders that just pile junk. But unless you know the places to look and understand what can and cannot be delete, this process will just be too much of a headache. Thankfully there are programs out there designed to do some of this work for us. CCleaner is a popular one that is pretty widely used and available for both Windows and OSX. It removes temporary Internet files, browser history, application caches, recent files, and much more. It also comes with the ability to wipe over the free space on your HDD to prevent forensic recovery of data. This comes in handy if you store sensitive files on your system or need to remain HIPAA compliant or the like. A tool that I commonly you alongside CCleaner on windows based computers is PrivaZer, which works in the same manor but with more features and better functionality. I suppose if I had to only install one, PrivaZer would be my program of choice. For those of you who fancy open source software, there is also BleachBit. Again, a program that works similarly but with different scan areas and items to delete. The shred levels are comparable between the three programs but I have found that using PrivaZer and BleachBit or CCleaner and BleachBit together gives me the widest scope for clearing out unneeded and unwanted files that could compromise my privacy and/or security. On OSX based computers, CCleaner is a good choice, but I have found that OSX stores a lot more "Hidden" information that you would expect. Some common folders to look in and delete files from are:

- /Users/Crypto/Library/Application Support
- /Users/Crypto/Library/Logs
- /Users/Crypto/Library/Preferences
- /Library/Logs
- /private/var/log
- /Users/Crypto/Library/Caches

You should be able to see all of the log files inside of "Console" and they can all get deleted on a regular basis. As well, the preferences files inside your User Library folder hold more information that you would expect. I found that about 50% of the programs I had installed were store recent file information in these folders. So when I was typing away and saving files in Text Wrangler, I was surprised to find that even though the recent documents were turned off from the File Menu, it was still storing the most recently opened file inside the preferences file.

It is also important that the drives containing your previous data are destroyed securely when they are no longer needed. Even if you are just moving from one computer to another, I would recommend starting fresh and only transferring the files over that are a necessity. Especially on

a Windows based computer, there are a lot of files that get stored in places uncommon for us to check. Even a simple thumbs.db file could be risky to our security if in the wrong hands.

There are typically two methods of making sure the data on these drives is not recoverable. Both methods take some time and aren't a quick solve so making sure all your drives are full-disk encryption is of great importance. The first one would be to take it out back and beat it to pieces with a hammer, drill some holes through the disks, and burn it. If the data on the drive was already encrypted, you can be sure an adversary isn't getting anything useful off it after you have shattered the disks to pieces. Do note though that Solid State Drives do not have disks in them and won't shatter the same. The second method of destroying sensitive information from your hard drives or external media (like a USB stick or SD Card) is to use a program like DBAN (Darik's Boot and Nuke), which is an open source software designed to be written to a disk or USB with the sole purpose of completely shredding all data from a device. It is often a good idea for Government Level Individuals to have a pre-made USB with the DBAN .iso written to it so you are ready to go when you need it. For maximum protection and to prevent any media being recovered, one could take their encrypted drive and wipe it with DBAN before reusing it. Or if you had no intentions of reusing it, you could then drill a hole or two into it and let your kid beat the sh## out of it with a hammer.

Edward Snowden?

The Final Section… Spoookie.
You might notice that the section header is "Edward Snowden?" with a question mark at the end. I did this because of my uncertainty with my ability to write a section dedicated to people needing his level of security. I'm not experienced enough and can really only comment on what I would were I in a position like his. So please understand that the next "category" here isn't at all from an experienced standpoint (that I am going to admit in a formal paper lol) and more-so from just someone whom has acquired some in-depth knowledge from reading online and befriending individuals with more security/privacy/anonymity related experience than myself.

Edit (April 27th, 2016): Spoke with one of the founders of IVPN over email today about ideas I had and the potential to introduce some of them into their company. During this email discussion, he made a VERY GOOD point about doing too much as a service provider to gain trust from your intended audience and then further discussed how companies that present themselves as providing *strong anonymity* can be a killer. This links in with my discussion about not trusting one service, company, product, etc with your life. They can very well do their best and even then that often won't be enough for everyone's threat model. Copy pasta:

> "I think there is a point at which it seems like you're pushing too hard for their trust which can be interpreted suspiciously. Clearly the ultimate goal is not to have to trust the VPN service but the requirement for trust is dependant to the threat model of the user. IVPN was never designed to provide strong anonymity, especially where the adversary has significant resources e.g. the ability to monitor traffic flow across large portions of the net (even Tor, a far more capable tool for anonymity is vulnerable to such an adversary). The vast majority of VPN users are not aware of the significant effort involved in achieving anonymity and promoting a VPN service as providing strong anonymity is careless and potentially dangerous in my opinion. IVPN was designed for privacy, specifically to counter the threat posed by the increasingly pervasive data retention laws and practices. ISP's are a credible threat due to them relaying all your traffic and they do retain records for various periods, in some cases by law. So when using a VPN, you're effectively trusting them not to perform any of those activities. However, this only requires that you trust them more than you trust your ISP. Given that a VPN's reputation depends on respecting customer privacy, not an unreasonable assumption."

The Issues With FOSS
Once you get down to this level, you almost need to reevaluate everything about your threat model and what you are doing to protect yourself. Even the littlest of things can bring a whirlwind of issues if you are up against the wrong people. Just in the previous section, we are discussing how open source software is a really, really good thing. And now, we need to discuss some issues with it and what you can do to combat these issues and stay safe.

FOSS is great because it allows us to look at the code in its entirety and verify that what we are seeing is doing what we are being made to believe it is doing. But in order for this to be a true statement, we need to understand everything about the published code. I for one do not understand how to code anything apart from a simple website in HTML so I have to rely on the word of others. This word is only as good as the people checking it though. So say we are planning on using ServiceX (just as an example) to communicate securely with someone else but ServiceX is pushing out updates on a pretty timely (monthly) basis. Unless we know how to read, understand, and validate the code ourselves, we need to have another trusted person who is able to do this. Furthermore, that person needs to be doing this when every update is pushed. Then we raise the question on whether one skilled person looking at the code is enough? If this person misses something that has the potential to compromise us, we would be using ServiceX up until the point and time where someone else does notice this fault. Even though that timeframe might only be a matter of days, those are days where everything we do in association with this service is compromised, which by association, compromises us and our entire model of security, privacy, AND anonymity we have worked so hard to build up.

Another issue with Free, Open Source Software is mobile platforms. On most operating systems for desktop computers, we can take the source code from the GitHub (or other code publishing website) and build/compile them ourselves if they have been written to work with our OS. But on mobile operating systems, we can't do that easily. And even in the cases where we can do it, we still face a huge challenge that doesn't yet have a magical solve. To download an application onto my iPhone, it needs to be published to the App Store by the company who developed said application. I can't go to the Open Whisper Systems website and download Signal straight to my phone. So even if we are checking the source code of the service/application (or having someone else do it for us), we still can't validate that the same application is being sent to the App Store for us to download. If the company was compromised by a body of law enforcement and forced to comply, they could publish a clean update to the GitHub, making slight UI changes to avoid suspicion, but then send a backdoored version of the same application to the App Store for thousands of users to download. This holds true in a sense for Android devices and the Google Play Store as well. The only way around this with the Google Play Store is to submit reproducible builds for the public to see and make use of. Open Whisper Systems has just pushed this out for Signal and it would be really nice to see other services do the same (Hint Hint: ProtonMail, Tutanota, ChatSecure) https://github.com/WhisperSystems/Signal-Android/wiki/Reproducible-Builds. So since we can't easily verify that the application we are using on our phones isn't doing malicious things, it should be a fair assumption that ditching mobile devices and using strictly desktop versions of programs, ones we can compile from source and monitor ourselves, is the best route to travel down.

Code Audits

Even after reading all of the above about Open Source Software, there still lays a huge issue that needs to be hurdled before we can be certain that the software we are using is secure. It isn't fair to assume that 100% of the people reading this section are going to be able to check through the code of an application themselves. Hell, it isn't even fair to assume that 5% of the people reading this could perform such a daunting task. Take TrueCrypt for example. The code

audits performed to make sure it was secure took months, from people light years ahead of me in the field of encryption; some of these people holding master's degrees in the area with years of experience under their belts (cough, cough @matthew_d_green). So assuming that one individual can do this sort of thing to keep his or herself secure is silly. Code audits on the applications and services we are trusting with our security at this level is crucial. And once this code audit is complete, you then have to consider that the audit won't be valid for further versions of the application. The second they send out an update and you install it, you have gone back to square one unless someone is viewing the changes and verifying them with every update.

Secure Operating Systems

Before we dive to heavily into the tactics that are going to keep an individual at this level secure from a big name adversary, we have to consider the operating systems that we are doing our work on, communicating through, and using to send people information. For reasons I shouldn't have to mention, you surely wouldn't want to be relying on Microsoft / Windows to keep you safe so I won't be discussing it at all here. And you really wouldn't want to rely on OSX either due to the fact that it isn't open source software and not developed with the complete security of the user in mind. So what operating systems are going to do the best job of:

- Keeping you as a person secure in the online world
- Making sure your information and data remains private
- Upholding a good level of anonymity to help defend you from adversaries
- Proactively defend against outside attack

Tails

As far as anonymity goes, the Tails Live OS, which was developed by The Tor Project is pretty much at the top of the chain. Although it is very restricted in what it can offer you, it makes sure that all connections to the Internet are routed through the Tor network so your real IP and location are never disclosed to a third party. It comes in the form of an ISO that you would write to a CD or USB. This makes it a tool you can take with you to remain anonymous anywhere you have access to a computer. Just boot the computer from your Tails USB and you are safe to browse the Internet, communicate with others, and share anything anonymously.

Debian

Taking away some of that anonymity and trading it for an operating system that gives great versatility in terms of security, Debian is my quick pick for a Linux/GNU install. Not only is it the operating system that is on all of my servers, it has done me good on my personal computers as well. Usually I would be partial to a distribution of GNU/Linux like Kali or BackBox that provides a lot of penetration testing and network analysis tools. However, the focus of this paper is defensive and not offensive so it didn't really make sense to me that I do a write up about BackBox, even though I would likely prefer it as a first pick install for Linux. The nice thing about Debian the ability for an individual to get full encryption of the partitions you are using AND use key files, which could be stored on an external device like a USB. See here: http://madduck.net/docs/cryptdisk/ for a tutorial. Debian is also an open source and very customizable operating system. They also provide an in-depth manual on how to secure the OS

properly: https://www.debian.org/doc/manuals/securing-debian-howto/ and there are tons of other tutorials available online about modifications and tweaks you can make to keep yourself safe. Unlike some of the other operating systems I have used, Debian is constantly being updated to keep the servers it is running on, and the individuals who are using it, secure and safe. And you can still do the majority of the things with Debian that these other operating systems provide. IP Tables or a similar firewall can be configured to only accept connections through the Tor network, VeraCrypt and TrueCrypt can be installed to create encrypted containers for even more security and privacy, and you can even separate sections of the US with permissions based controls.

Qubes OS

A fairly new addition (Initial Release in 2012) to the operating system community is Qubes OS. It was developed to be free, open source software that is secure from the core out. Unlike something like OSX or Windows, Qubes takes security to a whole new level and wasn't really developed for anything other than doing just that. It uses a unique approach called security by compartmentalization, which allows a user to isolate certain parts of their digital life into virtual machines very easily. This would give you the ability to do certain "activities" or "tasks" within an isolate section of Qubes so that even if that section were to be compromised, it wouldn't compromise the integrity of the entire operating system. You can read more about Qubes OS here: https://www.qubes-os.org/tour/#what-is-qubes-os and here: http://www.linux-magazine.com/Online/Features/Qubes-OS

Subgraph OS

As you can see from the write-up below, I had written about and was pretty happy to be including SubgraphOS into The Crypto | Paper. However, I had showed this OS to some friends of mine who are a lot more skilled than I am with computers, servers, reverse engineering stuff, etc and it didn't go so well. Nightfall (https://avac.io) explained to me: "Within 15 minutes Reiko (https://neko.li) and I had already broken it. Didn't even make it past grub and it ripped. Couldn't even install it without totally breaking it… it needs some work." I trust their judgment better than I trust most people online because I know first hand the skill Reiko has. He wouldn't recommend the operating systems from a privacy or security standpoint as of right now so I am keeping the write-up I did on it, but NOT RECOMMENDING IT FOR USE. If and when they can get it sorted out and have some skilled individuals put it to the test, I will be more inclined to remove the lines crossing out the next two paragraphs.

~~A very recent addition to the operating system community (early 2016) and one that has a very strong intent on personal security and privacy is Subgraph OS. It is another Open Source operating system that was designed to be very usable, comes security hardened out of the box, routes sensitive applications through Tor, and contains their own built in email client that has OpenPGP integration included. The nice thing about Subgraph is that it is almost identical to Tails in that a good majority of the OS is routed through Tor so all outgoing connections are anonymized, but it has the advantage of being a fully working operating system. As well, the installation of Subgraph requires that LUKS be used for Full Disk Encryption and the OS wipes the memory on shutdown to prevent against cold boot attacks~~

~~(https://citp.princeton.edu/research/memory/). It is really appealing to have an operating system that forces full disk encryption and takes an even further leap forward in wiping the memory to help protect this FDE.~~

~~Furthermore, Subgraph uses an application-based firewall by default that stops unknown and potentially malicious connections from "phoning home" by requesting user authorization on outgoing connections. This would typically work the same as LittleSnitch for OSX as described above. Alongside this firewall, applications are contained within the OS to be separated or "sandboxed" from critical parts of the system. Running inside a GRsecurity-enabled kernel makes sure that applications can't do malicious things like log your keystrokes, or have network access when they do not specifically need it. More information about Subgraph and the products they provide (like their secure operating system) can be found by visiting their website: https://subgraph.com/index.en.html~~

Virtual Private Networks & Tor

The issue once you get to need such a level of security that you find yourself categorized in a paper like this is you are really the only person who knows what you need to keep yourself safe. That presents an issue in itself because you are hopefully reading this paper to gain some knowledge. I however, am not the type of individual to be able to relate very well with you but I can tell you a philosophy a friend told me a few years back that has stuck with me since. "When you are literally fighting for your life online, NEVER put all your trust into one company or service". To attain maximum security, privacy, and anonymity, one needs to be sure they aren't putting all their cards down in one area and not focusing on others. An example of this would be just using the Tor network to attain Internet anonymity. This is an "okay" model to follow if we assume the Tor network is as secure as it is made out to be. However, recent events have unfolded that claim otherwise (http://gizmodo.com/judge-confirms-carnegie-mellon-hacked-tor-and-provided-1761191933). Instead, you could purchase 2 very reputable VPN providers like say IVPN and CryptoStorm, and then chain them together in succession before using the Tor Browser Bundle. You would need to be cautious that no IP leaks were happening in the process but say if you connected to the first VPN on your host OS and then ran Debian from a VirtualMachine, you would be able to connect to another VPN provider within the Virtual Machine and attain a very high level of anonymity and security. Not only would this really limit your attack vector, but it would be like making your own little Qubes by compartmentalizing that section and keeping it separate from the rest of your system.

IVPN provided a really great tutorial on using Virtual Machines, VPNs, and Tor together to acquire pretty complete network anonymity. I would highly recommend their "Privacy Guides" section of their website here: https://www.ivpn.net/privacy-guides/
These guides are very well written and provide a second perspective from my own.

Password Management & Storage

In the beginning sections of this paper, I talked a bit about creating strong passwords and how to store them securely. However, if your threat model fits you into this final category, you pretty much need to ignore all of that and redesign your system for password management. I

highly recommended LastPass because it is incredibly easy for all kinds of Internet people to use but also very secure from a malicious person trying to steal your information and identity. There are quite a few issues with LastPass when your life depends on security and privacy. The first of those issues being the fact that it isn't Open Source. Our data is stored inside a vault that is fully encrypted with our password, but we can't confirm that there are no backdoors because we can't see the source code for ourselves. Secondly, LastPass stores your passwords in the cloud and I would probably avoid all cloud-based password managers if I fell into this category of people. Lastly, what if they are provided with a subpoena or warrant for our information? Then what?

So to begin, we should probably consider my form of password creation that is available at https://cryptoseb.pw/passwords.png to be too "amateur" for what we need. The created passwords are secure, but they don't have enough randomness to them to give us a high enough level of security. Instead, I would recommend creating or generating passwords 19-20 characters of length for most of your online accounts, and 40-50 characters for services that are dealing with sensitive information/documents (SpiderOak, VeraCrypt, etc). To create this longer 50 character passwords, one should be using Diceware and adding in symbols & numbers at the beginning/end. An example of a strong random word password could be:

%[<Humming Greek slider for Timothy star@\@182

Something like this uses 5 randomly generated words and the connecting word "for" to make a fairly memorable sentence of them and adds some symbols and numbers to increase the strength. An alternative method I came across when doing some reading was to use the traditional Diceware method but to generate 5 words and put a symbol with 2 spaces in between each word. The result would be something like this:

good * waterfall / Cambodia ; finances ` again

You would be acquiring the password strength offered by the randomness of diceware, but adding to it by throwing in 4 symbols and 2 spaces for each one. But if you are the kind of individual who can remember a 35, 40, or even 50-character random password, all the power to you!

Since we shouldn't store our passwords in a cloud-based service, we need to look at getting one that provides the same security requirements, but keeps everything in a local format that we can encrypt. Probably the best password management software out there right now in terms of security would be KeePassX. Originally an application just called KeePass was developed (back in early 2000s), but it only worked/works properly on Windows based machines. So because of this KeePassX was created as an open source fork of the program in 2005. It uses either 256-bit AES or 256-bit TwoFish for the encryption of your KeyPass Vault, but because the file is portable, it can be stored on an encrypted SD card very easily. Like LastPass, it requires a master password for encrypting and decrypting the data but also allows a user to add a keyfile for added security (much like how TrueCrypt and VeraCrypt do). Because KeePassX doesn't need

access to any sort of a server with all the password management being done locally, you can firewall/block all connections to and from the program for added assurance. Check it out here: https://www.keepassx.org/

Encryption… Again

I know, I have already discussed different areas of encryption in varying levels of detail. But I think an aspect that needs to be highlighted even further is a point I made shortly above. "When you are literally fighting for your life online, NEVER put all your trust into one company or service". This applies to encryption on every level as well. Say you have a folder with 6-7 top-secret files in it and you need to make sure this folder is secure from all forms of compromise. You would want to make sure this folder was stored on a system that was completely encrypted and away from prying eyes. I personally would FDE a USB with VeraCrypt and a 45-50-character password. I would make sure the encryption algorithm was cascading like AES(Serpent). I would then mount the encrypted USB and place say 400 random files (pictures, random .txt files, etc) on the root directory. Then TrueCrypt would be used to create an encrypted container on the same USB using a different 50-character password and 3 keyfiles selected from the 300 images. The folder container sensitive information would then be stored within the TrueCrypt container on the VeraCrypt encrypted USB. To attack this setup, one would first need to break into the USB by attacking VeraCrypt; either by bruteforcing the password (not easily done with length of password), or attacking the encryption itself (which is also not happening due to cascading mode used). To put things bluntly, the FDE on the USB isn't getting broken into unless they can steal your password. Furthermore, this adversary would also need to then successfully break into the TrueCrypt container being stored on said USB. Another feat that is pretty much impossible due to the 50-character password and added security of using 3 keyfiles from a 300 choice lot.

When we take this same sort of thinking and apply it to securely communicating with someone, we should find ourselves looking for a method that would allow us to employ our own encryption over top of the encryption provided by the service we are using to communicate. Ideally, something like XMPP (using OTR and your own server of course) using Tor Messenger to keep things anonymous would be a good and secure method to communicate. On top of this, we could write our messages locally in a .txt document and then encrypt the text with the other person's PGP key before sending it to them. An adversary would first have to break OTR (Off-The-Record) or attack the client we are using AND crack the PGP encrypted messages. The OTR protocol should make use of perfect forward secrecy to assure that even if you lose your private key, no previous messages can be compromised. No matter what form of communication you use, I would make sure it employs strong PFS, and has an easy way to add a form of encryption on top of it (like PGP). I am with Snowden when he says that Signal is a very secure way to communicate with someone. BUT, one would ideally need a true burner phone that doesn't link to their identity or they have to give out their personal phone number to the other party. AND they need to be able to verify the source code on the device they are installing it on; a feature that is not yet available for iOS.

Where to Communicate

You might never think of physical security coming into play too much if you have a very high level of Internet/Device security. But it is actually a lot more important than one would think. If we are "important" enough to need the security online, we definitely need the security in real life. So the question to ask ourselves is: "where is an acceptable places to communicate securely with another party." One might think that the comfort of their home would be the best place to do this but I would argue against it. I argue against this because it isn't difficult for a skilled adversary or Government level body to place physical tools for spying (like cameras or hidden audio recording devices) inside of the places you frequent. They break in when you aren't there and hide devices meant to capture your every word. If this were to happen, and then you held a very private conversation over Signal with another individual, your entire conversation may be compromised. Jumping onto the other side of the fence, if you are going somewhere very public and not someplace you frequent often to do the communicating, like a coffee shop, you also have a fair amount of physical obstacles to jump. Being careful that people are not recording you in that setting is likely even more difficult and most of these places would have cameras that you need to be avoiding.

So how do we acquire the "perfect place" to communicate with someone else? The best answer I think is: in person. Meeting up with someone in person has the added benefits of not needing a bunch of digital security but it comes with the drawback of ease and usability. It isn't always easy to just meet someone and have a private conversation with them. You also need to be in complete trust with the person you are meeting. If they turn out to be an adversary under cover, you could have your entire model of security destroyed in seconds. But what if we did the communicating digitally from a location that was removed from our personal life, not very public, and only semi-permanent. An example could be an apartment you are purchasing with cash and a fake name (to keep your identity anonymous). You could take a different route to get here everyday to avoid being followed by anyone, and make use of tools like bug sniffers (http://www.spytechs.com/bug_sweep_equip/) to make sure the space around you is clean from digital recording equipment. Because this location is not common to your real identity, it isn't easily compromised.

One thing you should be cautious of though when employing methods like this is how our devices can track our every move if we aren't careful. Having our phone turned on could disclose our every move to someone who is able to track it. Even an installed application with too many permissions could reveal our location. So keeping your mobile devices under a strict watch is good, but turning them off and considering a Faraday Bag to stop all ingoing and outgoing signals from the device (https://www.amazon.ca/Black-Hole-Faraday-Bag-Isolation/dp/B0091WILY0) is even better. Seems like a spookie thing to do but Farday Bags and Cages are very common tools for law enforcement that want to make sure devices stay in the state they were taken in. Nico Sell, the Founder of Wickr, talks about "Tricking Google Maps" and providing disinformation Online (http://www.dailydot.com/technology/online-privacy-tips-from-wickr-ceo-nico-sell/). I'm not the only one promoting these "crazy" ideas and I am sure it isn't just the two of us either. Geolocation is a killer and many of the services you use, alongside your mobile device, are lovers of it.

Data Integrity

Pretty much the only thing left to do is to make sure that our data is not being changed or altered without our prior knowledge or consent. We can do this on our systems by using what is known as File-Change Detection or Integrity Monitoring Systems. They are very common server-side but also important to consider for your personal systems as well. These applications/services for your system work by monitoring certain files or sections of your system for any sort of read or write changes. So if we had a system like this configured on our server and someone were to break into it without our permission, we could be alerted by email if certain files were to be accessed or changed. This would give us a heads up that one of our systems has been compromised.

I am not really an expert in using these types of tools but I have done a bit of reading on them and have found 2 popular ones that you can do your own research into.

- OSSEC - https://ossec.github.io/
- Tripwire - https://www.tripwire.com/solutions/file-integrity-and-change-monitoring/

As a side note, I have a friend who has developed a rootkit that is able to bypass OSSEC in its default state on Debian 7. I am unsure on whether this works on a Debian 8 system but can confirm that it is NOT streamlined for any other OS. The reality is that even with File-Change Detection Systems, it is still possible to completely roll your system onto its back if someone is experienced enough. Nonetheless, adding these security measures into your setup isn't a bad thing and will only work to increase the security you have. For further reading see: https://www.digitalocean.com/community/tutorials/how-to-use-tripwire-to-detect-server-intrusions-on-an-ubuntu-vps and https://www.alienvault.com/solutions/pci-dss-file-integrity-monitoring.

Emergency Preparedness

If we were to place security, privacy, and anonymity onto a sliding scale from 1-100, nobody is going to be able to achieve all 100s. It is just not feasible to attain a perfect score of safety. Knowing this, we need to be ready for the "What ifs" and the scenarios when shit hits the fan and we are literally dealing with the repercussions of something serious. I'm not going to comment on what may have gotten you into this position, but I will try and help you get out of it.

For starters, this entire section (like most of what is included in this Edward Snowden? category) is going to be speculation. I would love to give you so much more information and write without restrictions, but my safety has to be included. I'll leave it at "legal".

We have to think about what might happen in the worst possible scenario and then REALLY think about what would happen in that scenario. Maybe it includes a swat team and the sentence "You have the right to remain silent…" or maybe it just means getting fired from your job. In any situation, it is important to think ahead and have a plan of action ready for when you need it.

The first step I think is going to be revisiting (AGAIN), how important Full-Disk Encryption is on your devices and being able to turn those devices off in a hurry. A device that is properly encrypted is the strongest when it is off. This also includes your mobile devices, but thanks to Apple, your iPhone is already secure even if it is powered on; so long as it is locked of course. A few pages above, I talked about DBAN and how I always like to keep a USB formatted with it handy for those "just in case" scenarios. It isn't going to be a quick wipe by any means, but at least with a fully encrypted drive, you could just pop in the USB, set it to wipe everything, and leave. You wouldn't have to worry about someone halting the process because your drive was already full disk encrypted to begin with.

Another neat tool that you should check out is "swatd". I won't do really any explaining about it and leave all the reading/research up to you but will say this. Imagine what you could do with this program and some cameras in your computer room? See: https://github.com/defuse/swatd and https://thetinhat.com/blog/2015/01/24/get-swatd.html

But what are the consequences of actually going through with a tactic like this and purging all of your data. You would literally lose everything on the devices you wiped! This includes things like your PGP Keys, SSH Keys, and encrypted containers. In knowing this, it might be a good idea to have an external hard drive that is fully encrypted where you can backup a lot of crucial files every month and then store it in a secure place (maybe even off location incase the unthinkable does happen). You could also consider encrypting your sensitive files in say a VeraCrypt container or with your PGP key and then backing up those files to a cloud service. This would give you access to them virtually anywhere as long as you had access to a computer where you could install VeraCrypt. If you chose to encrypt them with your PGP key, it might add some security, but wouldn't be as easy to decrypt them if needed (taking into account that your private key would have to be backed up somewhere completely different).

Conclusion

Finally, I am able to say that The Crypto | Paper is complete! It is a huge achievement for me to say that. Writing this paper has taken countless hours, lots of research, and one too many discussions with people who have more knowledge and experience than myself. One of the older fellows that I have nightly coffee with made a comment to me that it was nearly impossible for him to keep up with the advancements we are making in technology and the way he talked about it, it was almost like he was just trying to stay afloat. This hit me as rather concerning. If we are moving this fast into a digitized world, where will my parents be in 5, 10, 20 years time? Would they be able to keep up? Or would they feel just as helpless? I got a lot of the inspiration for writing this paper from the amount of people I talk to who have zero clue how to keep up, stay secure, and even properly run a business in our Internet world today. But because I have been involved in, and always really interested in learning about security, privacy, and anonymity, I wasn't just going to stop with the basics. I have had a fair amount of previous experience with the areas covered in this paper. So I figured it would be a great challenge to take on and I definitely had fun.

Even if you were only able to get through the first category/section before being completely lost, I hope you were able to take something away from The Crypto | Paper. And if you made it all the way to the end and had some concerns with things I have written about or views that I have, I encourage you to get in touch and discuss them with me. I mentioned in the introduction that this is largely a construction of the experiences and knowledge I have had and acquired over the last few years being a part of this "scene" so I know it will definitely not be perfect. Everyone who is well versed in these fields will have their own views on the topics discussed and many will have a lot more knowledge than myself. So if you are one of these individuals, please don't be shy. Out of all of this, I want it to be a learning tool for not only those reading, but also myself. I will work on and improve this paper as I have time and as I receive criticisms and suggestions.

Please feel free to contact Blake or myself with any and all concerns, questions, or feedback. We look forward to hearing from you! **Official Subreddit:** https://reddit.com/r/cryptopaper

Thanks so much for reading. I encourage you to link to this paper, print it off, share it in any way you see fit. Just please do not alter the paper in a way that would discredit the many hours I have put into developing and writing it and the many hours others have spent reviewing it before it went public.

Crypto | Seb

Resources For Further Reading

Note: Some of the links were too long to fit on one line, which took the nice flow away from the formatting. I have replaced the longer links with a shortened URL from Windscribe's Secure.Link service. When you click the secure.link URL, it will take you to a page where you can preview the webpage before being redirected. This removes the possibility of someone redirecting you to a malicious site or download. Because some of you carry a much more intensive threat model than myself, you should consider "URL Expanders" to check that each and every link is clean. **Don't trust me if you don't know me**. I am just some random guy who wrote a 61-page paper in his spare time. Blake wanted them removed but I stuck with my counter argument that it is good for those reading the paper to understand the implications of a "bad/malicious" link and how to properly view one without infecting yourself.

PrivacyToolsIO - https://www.privacytools.io/

VPN Comparision Chart - https://secure.link/YPwJM7Rt

IVPN Privacy Guides - https://www.ivpn.net/blog/privacy-guides

OSX Security Guide - https://secure.link/gdB1Zw5J

Electronic Frontier Foundation - https://www.eff.org/

Crypto World - https://cryptoworld.is/

Defuse.ca - https://defuse.ca/

OpenSSL Name Mapping - https://testssl.sh/openssl-rfc.mappping.html

SSL Test/Scan - https://www.ssllabs.com/ssltest/

IM Observatory - https://xmpp.net/

VPN Anonymity (2016) - https://torrentfreak.com/vpn-anonymous-review-160220/

Infiltrate The Vault - https://eprint.iacr.org/2012/374.pdf

FileVault2 Analysis - https://www.cl.cam.ac.uk/~osc22/docs/cl_fv2_presentation_2012.pdf

Open Crypto Audit (TrueCrypt) - https://opencryptoaudit.org/

Panopticlick - https://panopticlick.eff.org/

SSL Browser Test - https://www.ssllabs.com/ssltest/viewMyClient.html

eCryptFs Audit - https://defuse.ca/audits/ecryptfs.htm

/r/privacy - https://www.reddit.com/r/privacy

Shitlocker - https://www.schneier.com/blog/archives/2015/03/can_the_nsa_bre_1.html

Privacy101 - https://www.privacyinternational.org/privacy-101

iOS Security - https://www.apple.com/business/docs/iOS_Security_Guide.pdf

iCloud Security - https://support.apple.com/en-ca/HT202303

Creating Strong Passwords - https://support.apple.com/en-ca/HT202303

Metadata - https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.asp

ZeroBin – https://cryptoseb.pw/message

Let's Encrypt - https://letsencrypt.org/

CryptoCat - https://crypto.cat/

Tor Project - https://www.torproject.org/

DNSLeakTest - https://dnsleaktest.com/

Canary Watch - https://canarywatch.org/

Surveillance Self-Defense - https://ssd.eff.org/en

Reset The Net - https://www.resetthenet.org/

Blockchain.info - https://blockchain.info/

Prism-Break - https://prism-break.org/en/

Watched - https://theintercept.com/2015/07/14/communicating-secret-watched/

Footnote *: I, Phone - https://www.youtube.com/watch?v=e-ZpsxnmmbE