Please note that the following is a draft document, most of which was transcribed from pages handwritten in pencil while the author was residing in Maplehurst Correctional Centre during 2010 & 2011 on G20 related charges. As such there may be spelling and grammar errors present.

Please spread this document around. Please consider modifying this document to include your own information. Attribution to the author, Byron Sonne, would be appreciated but is by no means necessary. Keeping activists secure and safe is a far more important cause than any one person.

This is Revision 3

SECTIONS

Security and Encryption Basics and Philosophy

Your task is to make your adversaries spend as much effort, time and money as possible in breaking your security. Keep this in mind at all times!

To make them expend effort, encryption is used to keep information secret. But to properly appreciate encryption you must be familiar with something that is known as Kerckhoff's Principle (http://en.wikipedia.org/wiki/Kerckhoffs's_principle).

A more concise explanation is no doubt available, but put simply, this is what it means: a truly secure cryptosystem can have all of it's innards exposed and still be completely secure. Even if the algorithm is known and laid bare it does not matter – this gives zero edge or advantage to someone trying to crack the code. The KEY – password or passphrase – is where the true security lies. The key cannot be factored from, or determined, via the algorithm. All of this, of course, assumes the algorithm has no flaws.

Contrast this with practices summed up by the phrase “security by obscurity”. Parties practicing this rely on their adversaries to remain in perpetual ignorance in order to keep things secret. But as soon as the secret info is guessed (or even determined accidentally) all security is lost. It is like hiding something under a rock and praying that no-one decides to look there.

If an algorithm is weak (or flawed) it is foolish to employ obscurity as a means of bolstering its security. Sooner or later a devoted adversary will discover the weakness and all security predicated upon it is rendered void. ZERO SECURITY IS BETTER THAN FALSE SECURITY!

These concepts, taken together, illustrate a key assumption one must begin with when employing encryption. You must always assume that your adversary will obtain a copy of your data in encrypted form and will know what algorithm was used to encrypt is. Thus the key piece of information that must be kept secret is (of course) the KEY – the password or passphrase used.

The key must be kept in your mind and never written down. It is a challenge to generate, pick and commit hard-to-crack keys to memory, but it must be done. If you store keys by writing them down then you can effectively reduce the most secure cryptosystem in the world to mere “security by obscurity.” All someone has to do is find the written down key and ALL is lost.

A third concept sets a practical limit to the implementation of perfect (or strong) security. We'll call this concept “Rubber Hose Cryptanalysis”. What this means is that even with the best encryption theoretically possible, if your adversary can't crack your encryption, then they'll simply employ violence or torture and, quite literally, beat it out of you. One person employing physical coercion is far more effective than the sum of National Security Agency or governmental computing resources if they want what you've hidden.

This brings a fourth concept into play – encryption should be considered a delay mechanism and NOT an end goal of perpetually uncrackable security. Sooner or later, one way or another, your adversaries

will get access to your secrets if they're motivated enough. This is the salient point: IF THEY'RE MOTIVATED ENOUGH! Again, it's your task to make them spend as much time, effort and money as possible. If you live in a decent society then it's likely you won't be tortured into giving up your keys. If this is the case (and lucky you!) then it's technically feasible to encrypt information so that your lifetime, and those of your adversaries, will elapse before your secrets are decrypted and revealed. If it's possible you'll be tortured into giving up your keys, then you need to consider whether it's worth the risk to commit your information to media at all. Keep it all in people's heads and employ additional means – dispersal in parts? - to make it harder to get at.

Given that it's your task to make your adversaries spend as much effort, time and money as possible to decrypt your data, you need to be aware that this goes both ways. This is a fifth concept to heed: that of trade-offs.

Security and encryption are, by their very nature, inconvenient. If it's a hassle for your adversaries to decrypt it then you must assume there will be some hassle in encrypting it. A balance needs to be struck – if it's too much hassle people will forgo the process and avoid using encryption at all. If they MUST use encryption and it's a hassle, then users may jeopardize security by resorting to writing keys down – and then you're back to “security through obscurity”, the worst kind.

You need to consider, and determine, how much of your information needs to be protected. Is it static or seldom changing repositories of information? Then it won't be so inconvenient. Is it high volume, near constant streams of interpersonal communications? Then it's likely going to present some annoyance at regular intervals. Some of this annoyance can be “paid up front,” in the work that goes into installation and initial configuration. Annoyance will still be had during regular use—for instance, having to enter a key to decrypt each newly arrived encrypted email. And you'll need to do this: NEVER store or cache keys so you only have to enter them, say once on start-up of your email client. You never know whether your 10 minute trip to grab a coffee is just that, or whether you're under surveillance and will be arrested as soon as you step outside, leaving all your email at home, decrypted and readable.

This leads into a sixth concept: information you wish to keep encrypted needs to stay encrypted! Don't leave your “secret sauce” out in the open—if you don't need access to your encrypted files then don't decrypt them. It's simple: decrypt the information, do your work on it, and as soon as you need to take a break or are finished, re-encrypt it. Make sure your backup system backs up only the encrypted information. If you run continuous backups, such as with Apple's Time Machine, then stop or pause the backups when the information is in a decrypted state. Furthermore, lock your machine—or preferably logout and power off when you're away from it. At the very least, lock your screensaver. Also unmount any USB keys and ensure they are also in an encrypted state before leaving the vicinity of your machine.

As a mental exercise, consider that at any moment you are going to be abducted right out of the very chair you are sitting in, and your equipment seized. How must you operate—what are your workflows and methods?—to ensure that as much information as possible stays encrypted, assuming that you'll have zero time to activate various encryption and security mechanisms before the door is kicked in and you're wrestled to the ground and cuffed? Paranoia is a virtue when security is in your interests!

Develop scenarios based on such possibilities and role-play them in your mind (or in real life) to test your responses and ensure that they actually deliver the results you need. If you're using a laptop or netbook computer, how quickly can you force it to power off completely? With a regular computer, will yanking out the power cord work, or will it result in a damaged operating system and files? Just as importantly, will an emergency power-off result in an insecure state when the computer is turned back on? Check and confirm that no secret and decrypted information is left hanging in aborted or scratch files or applications. For instance, maybe you used Microsoft Word to write a document stored in a TrueCrypt secured volume, but subsequent to an emergency power-off (and upon reopening Microsoft Word) you might find that Word saved a copy of the file to another location as a safety measure—trying to be nice by saving you from losing work.

The time to implement security and encryption is not when you are under duress. Security is a process, not a static state or thing that you lack one day but have the next. It affects every aspect of what you do, and so you need time to integrate it into your processes and workflows. Many of the tools take time to learn, and to gain maximum utility from them familiarity via constant use is required. Practice makes perfect!

You must begin to use these tools and implement the processes NOW so that when crunch time comes there is no discernible increase of effort required. If you wait for the last minute you'll be stressed out and will make mistakes. Furthermore, there is a counter-intelligence benefit initiated against your adversaries by implementing encryption and security far in advance of operational initiatives or actions. It serves to thwart “traffic analysis” (http://en.wikipedia.org/wiki/Traffic_analysis)—this is a method of intelligence gathering whereby changes in the quantity or quality of communications are used to draw inferences about current or future activities. Sudden deployment of encryption and enhancement of security close to the date of an action throw up big flags that say, “Something's about to happen, get ready!” But, if you implement well ahead of an action, you deprive your adversaries of the intelligence benefit of being able to correlate changes in traffic to changes in plans or activities.

This must be taken a step further to gain maximum tactical and strategic advantage. The change in volume of communications must not appear to increase or decrease in proximity to an action. One of the first things your adversary will do when monitoring your communications is to baseline the quantity and destination of messages.

As an example of thwarting such traffic analysis, suppose that 100 messages are sent weekly between users. During “down time” or between actions, only 10 percent of messages may contain content that is useful or of concern to you; let the remaining 90 percent be convincing filler that is also encrypted so that your adversaries cannot read it. Keep up this pattern for a long time and soon 100 messages are the “baseline” and not considered odd. As the date of an action or operational initiative approaches, you now have a buffer of 90 messages that can be used to relay important information, and nothing from the outside appears to have changed—the same 100 messages are being sent.

An additional benefit is gained from this: your “useful” traffic is mixed in with much more “filler” which makes it harder for your adversary to determine the signal from the noise. With more traffic to analyze, and more encryption to try and crack, you're now forcing your adversary to spend more effort, time and money. Your task is to sap their energy and increase their chances of making mistakes.

Security “Bang for the Buck”

Some fairly easy and inexpensive steps can be taken to raise your security “threshold” immediately. Those steps, in no strong order:

1. Turn on any “boot” options for passwords in your computer's BIOS/EFI. This way, when your computer is powered on your adversaries will have trouble accessing the operating system. However, this can be circumvented by removing the hard drive and booting it using another computer with no BIOS/EFI password. But remember: your task is to force your adversaries to spend as much effort, time and money as possible. Give them a hassle!

2. Require a user account and password to login. Avoid auto-login at all costs. Do not give your adversaries the gift of a wide open desktop just by pressing the power button!

3. Set a password on your screensaver, and make it a good one. See if some kind of hot-key or mouse gesture can be configured so that you can engage the screensaver with a quick and easy motion. Make it easy on yourself. Always engage your screensaver when you leave your work area.

4. Turn on file system encryption options—these exist for OSX and more recent versions of Windows. When you are not at your machine, log out and power down. This way you have multiple levels of protection—encrypted directories/drives and the requirement of a password to login.

5. Install TrueCrypt (http://www.truecrypt.org/ Windows, OSX, Linux) and create a few encrypted TrueCrypt volumes. Move all your documents into these volumes—at least the sensitive ones. If you have already implemented encrypted filesystem options, then you should still implement some TrueCrypt volumes. This gives you a second level of encrypted protection. DO NOT USE AUTOMATIC MOUNTING OPTIONS! Ensure that mounting encrypted partitions or folders requires full manual intervention.

6. Investigate all the programs/software on your machine—especially that which you use—and disable all “history” and logging functions. This is especially true for chat/IM clients. It may be convenient for you to be able to scroll back to see what you or others have said in the past; rest assured it's even more convenient for your adversaries!

7. Don't keep your email stored in your email client. Erase it after sending/receiving it and using it. If you must hold on to it, copy its contents and save it as a file in a TrueCrypt volume.

8. DO NOT USE WEBMAIL SERVICES or store you email on GMail/HotMail/etc. servers. All your communications must stay resident on your machine where they are under your control and security. Use Thunderbird and implement encryption using PGP/GPG and the Enigmail add-on.

9. Install and use ad-blocking and flash-blocking software on your browsers. Disable caching and password saving. Disable web browsing history. Don't visit sketchy sites. Switch to Firefox instead of Internet Explorer. If using a Mac, turn on 'Private Browsing' in Safari. (https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/, https://addons.mozilla.org/en-US/firefox/addon/flashblock/, http://www.ghostery.com/)

10. Switch away from Microsoft Windows—since it has the largest market share, most viruses and attacks are targeted toward Windows. Switch to a Mac running OSX or use Linux.

11. Turn off your computer when you are not using it. If it can't be accessed then it is much more secure.

12. Turn on firewalling features. Turn off file and printer sharing features. If people can access your machine over the network then they can attack you. The only inbound connections to your machine should be responses to queries you initiated. Your computer should be as hidden as possible on the network.

13. Eliminate all use of wireless keyboards and wireless mice. Replace with wired versions. It is possible to “sniff” these exchanges, and even if they are encrypted, crack it and capture data.

14. DO NOT USE WIRELESS NETWORK ACCESS – EVER! Disable the wireless radio in your computer and in all your hubs and switches. Use only wired connections. This is for two reasons: (1) Your data, even if encrypted, can be “sniffed” and broken, leading to compromise; and (2) Even if encryption is not broken, “traffic analysis” can be performed and useful inferences drawn from patterns of wireless use. Turn off Bluetooth and IR too.

If you must use wireless access, such as from a coffee shop etc., considering acquiring a cheap portable machine such as an Asus EEPC netbook (http://ca.asus.com/en/Eee/) or similar. Avoid using it in a manner, or accessing sites, that will generate identifiable information. This machine should be used ONLY for wireless access and you should create different user profiles and passwords than those used on other machines. When you are at home you are one person—but when you are in public using this machine you are an entirely different person. If possible, acquire this machine from someone with no ties to you. Pay cash. This way, if you are compromised, you can dispose of it, or get up and walk away, leaving it behind, without any fear of it being tied to you.

After every sortie with this machine, consider a complete reinstall to a clean, initial state. Much the same effect can be accomplished by booting the machine from a non-writable media such as a CD or DVD running a custom Linux distribution, such as BackTrack (located at http://www.backtrack-linux.org) or EEEBuntu (AKA Aurora located at http://www.eeebuntu.org) when you are out. This way, a quick power off results in all of the data and environment being lost.

Secure Passwords and Phrases

Learn to live in fear of anything that requires eight characters or less as a password or PIN.

A good password/passphrase will contain upper and lower case letters, numbers and symbols. If you can use only an eight character password for a service or site (and if so, shame on them!), then "p@S$W0rD" is certainly better than "password"!

Your password must certainly NOT be a plain dictionary word; it is absolutely commonplace for automated password guessing software to be supplied with (aptly named) dictionary files. These may contain every word extant in the language of your choice. If such files are not supplied (they are often very large) then they can easily be obtained on the Internet for free.

Furthermore, your password or passphrase needs to be long and of mixed characters—letters, numbers and symbols—to complicate attacks based on the use of "Rainbow Tables" (http://en.wikipedia.org/wiki/Rainbow_table). The concept of Rainbow Tables needs more explanation. Good security practice means that passwords are not stored on a system in plain text form. Instead, passwords are processed using something called a "hash function" (http://en.wikipedia.org/wiki/Hash_function) —a mathematically irreversible process which yields a number. This hash function is "one way": there is no way to obtain the original password from this number.

The only way to figure out the password is to systematically generate every possible password, then "hash" it and compare the guess hash to the target hash. If the hashes are equal, then the two passwords must be the same. However, to iterate through all possible password combinations, hash them, and then compare them would take enormous amounts of time. Such an attack is referred to as a "brute force" attack (http://en.wikipedia.org/wiki/Brute-force_attack).

Rainbow Tables get around this problem because they are pre-computed sets of data: a very large collection of hashes of all possible password combinations for a given password format and length. Then it simply becomes a speedy matter of searching for the hash in question, which then of course reveals the actual password.

A Rainbow Table for a password that is one to eight characters long and consisting only of upper case A-Z will be far smaller than one that has been generated for passwords with a minimum length of 16 characters and composed of A-Z, a-z, 0-9 and symbols. A rainbow table for this password pattern would be impracticably large and take very long to generate. Remember: you goal is to force your adversaries to spend as much effort, time and money as possible. Don't make their job easy.

To drive this point home, consider how many permutations exist for the following patterns:

A-Z	8 characters long	$= 26^8$
A-Z + a-z	8 characters long	$= 52^8$
A-Z + a-z + 0-9	8 characters long	$= 62^8$
A-Z + a-z + 0-9 + symbols	8 characters long	$= 95^8$
A-Z + a-z + 0-9 + symbols	16 characters long	$= 95^{16}$
A-Z + a-z + 0-9 + symbols	32 characters long	$= 95^{32}$
A-Z + a-z + 0-9 + symbols	64 characters long	$= 95^{64}$

At bare minimum, passwords ought to be 16 characters long and composed of A-Z, a-z, 0-9 and symbols. If passphrases are a choice then opt for a bare minimum of 32 characters comprising the aforementioned character set. An even better choice is 64 characters long, and not that hard to remember if you choose a line of song or poetry. Choose a memorable line and then permute a few characters and inject random symbols. A or a become @; e or E become 3, s or S become $ etc. Even with such minimal permutations, when used in tandem with a long passphrase, your adversaries will be forced to dedicate significant resources to cracking your password or passphrase.

Police and Intelligence Agencies: Observations

Here is a basic and somewhat inaccurate mapping of Canadian and American agencies and how they relate, as well as their general areas of operations. This is, of course, not exact, and things may change in the post-9/11 climate. More work needs to be done for this section. A more comprehensive list of agencies worldwide can be found at http://en.wikipedia.org/wiki/List_of_intelligence_agencies.

Canada	**USA**	**Areas of operations**
Royal Canadian Mounted Police (RCMP)	Federal Bureau of Investigation FBI	Domestic investigation Powers of arrest
Canadian Security Intelligence Service (CSIS)	Central Intelligence Agency (CIA)	Foreign & domestic investigations No arrests
Communications Security Establishment Canada (CSEC)	National Security Agency (NSA)	Signals intelligence, code breaking
Integrated National Security Enforcement Teams (INSET)	Department of Homeland Security DHS	Coordinating/funneling agencies

Each province and large municipality will also likely have an agency present containing local police officers who are “seconded” to another higher agency. These “seconded” officers or agents are intermediaries who serve both agencies and ensure communications between their primary agency and their seconded agency are timely and effective.

For instance, in Toronto, the Toronto Police Service (TPS) has officers seconded to INSET, which in an Ontario provincial context may be referred to as OINSET. Additional agencies may also be present such as Joint Intelligence Group (JIG) for events such as the G20 and similar. The mandates of these agencies are, again, the timely collection and sharing of information between municipal, provincial and federal police agencies and national intelligence agencies. There are, of course, other agencies that may participate, whether they are military intelligence agencies or even more secretive, unknown agencies and unties.

The names of the agencies and what, exactly, they each do are not as important as realizing that such a structure exists. Municipal police forces will have access to national security bulletins and intelligence. Be aware of this. However, as one can imagine, such bureaucracy has its perils. For every person added, for every agency through which information has to flow, delays and errors may be introduced. Furthermore, the level of technical expertise of many officers and agents is of variable quality and usually low. That means that well thought-out security precautions and the use of encryption are very useful protective measures. Technical forensic units are almost always deeply backlogged, of course dealing with the most pressing concerns first. Don't become that pressing concern!

However, *never* assume that you are up against idiots. Always assume that your adversary is more intelligent than you. Remember what Sun Tzu said: *It is said that if you know your enemies and know*

yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.

One side effect of the generally low technical abilities of the officers and agents is that things will either fall through the cracks or be strongly overreacted to if they don't understand them. The sudden deployment of encryption may thus bring attention you did not previously have, as many officers and agents truly believe “if you're not doing anything wrong, why are you hiding things?” That they think this is truly deplorable and one reason for the sad state of our country and our civil liberties, but it's a reality that must be acknowledged.

These agencies, due to human resource limitations as well as technical abilities and legal concerns, employ a mix of measures against persons of interest. It takes a long time to find, hire and train people, and they are often overworked. Hence the use of informers, as planting a real undercover agent is an expensive and complicated measure. Yes, it does happen, but the likelihood is far stronger that a civilian, either a recruit for ideological reasons or a comrade turned rat in exchange for a legal deal, are far more likely to be the mode of human intelligence employed against you. Police officers like to go home at night, but that new roommate of yours could be an informer.

Physical surveillance is entirely likely. As most people do not think they merit such attention, officers may not do a particularly good job of it. For instance, if you maintain a regular bedtime and persist in this pattern for some time, surveillance may be called off once you are perceived to have gone to bed. Surveillance is boring, uncomfortable work for agents and officers and takes a lot of human resources. Monitoring the location and movements of just one person of interest, in at least one case, required nine people divided into multiple teams, relieving each other in variable length shifts as appropriate. This took place over a five day span and the person of interest was still lost in crowds and at subway stations.

You must, however, not rely or count on spotty surveillance. If your adversaries are truly committed to surveilling you, and are appropriately trained and motivated, you will likely never even know you are being watched.

Surveillance agents are also interested in determining the sorts of purchases you make and will go as far as following you around stores to determine what you are looking at or purchasing. They are also content to wait until you have left, after which they then ask the store owner or employees for information on your purchases. Again, due to generally low technical skills combined with ideological slants, innocuous items that you purchase may be misinterpreted and a context or story woven around them which is damaging to you.

For these reasons (and others) it may be worth the risk to make your purchases via other parties of preferably minimal relation to you, and with cover reasons provided. It might even be worth it to arrange for a stranger to go in and buy something on your behalf. In any case, consider proxying your purchases and have that person store it for pick up at a later time at a secure as possible location. Cash only, of course.

Paper Shredding and Media Destruction/Erasure

It is to your advantage to shred any and all paper—documents, bills, whatever—before disposal. One piece of apparently innocuous paper may do little, but many pieces can assist your adversary in determining patterns. “Traffic analysis” of a sort may come into play: your adversaries will develop a baseline of of your disposed paper, and a sudden change in quantity or quality can be used to draw inferences. Receipts from coffee shops, stores you frequent etc. can all be used to assist in surveilling you or placing you near or at a location you would prefer not to be placed. Pay cash and shred receipts.

The type of shredder used is important—any shredding is better than none but a “crosscut” shredder is superior to the average “strip” shredder. A crosscut shredder reduces paper into something resembling confetti. Regular strip shredders are far more common and cheaper and some can also shred CDs and DVDs and may be worth purchasing for this reason alone. But strip shredded paper, believe it or not, can still be pieced back together into complete, or nearly complete, documents. This takes a great deal of work and it is unlikely your adversary will go to this length, but it must be taken into consideration. Remember: your task is to make your adversary spend as much effort, time and money as possible.

It is worth burning all your paper as well—forensic analysis of paper, ink and fonts may be used to link you to documents you print and distribute. Destruction of toner and ink cartridges must be performed as well. Furthermore, printers of all types may leave unique signatures on the documents they produce, such as scrapes, marks etc, so consideration must be given to the destruction and disposal of printers if they are used to print sensitive materials. Printers are cheap enough nowadays that they may be purchased for a single run of documents and then disposed of securely.

As regards magnetic media such as floppy disks and magnetic tape, bulk magnetic erasure is insufficient. Methods exist to regenerate data on all varieties of supposedly wiped tapes or disks. These media are best disposed of by removing them from their plastic shells and cutting into small pieces, then burning or soaking in an appropriate solvent to destroy their structure. Merely unspooling a tape is insufficient as it can simply be rewound onto a blank spool for data recovery.

You need to perform these actions to counter something referred to as 'data remanence': http://en.wikipedia.org/wiki/Data_remanence.

Hard disks are best removed, opened up and the platters exposed to extreme heat (such as from a blow torch) or acids if you are in need of quick destruction. Otherwise, utilities/programs exist (such as DBAN—“Darik's Boot And Nuke” Linux distribution http://www.dban.org) that you burn onto a CD and then boot from. You will be presented with options to perform secure wipes using various methods —some of them being RCMP or American DoD specifications. This, however, can take *many* hours so plan ahead and take this into consideration. Practice secure erasure of files and media ahead of time so you know how much time it takes and what to expect.

Non-Electronic Exchange of Data

If you meet someone, say at a café, to exchange information or engage in discussion, it is easy enough for your adversary to eavesdrop and record the audio. Audio is much more omni-directional than video—so rather than talking, write it down on small pieces of paper and keep your mouths shut. It is a challenge for an eavesdropper to aim a camera of sufficient resolution to capture what is being written. If the person you are meeting is a potential informant it will also be difficult for them to capture solid evidence—photos of the writing—without engaging in suspicious behaviour.

When the exchange is complete, burn the small scraps of paper or tear them into confetti and flush down the toilet in the café, or chew and swallow them if necessary. Clearly this technique is most suited for small amounts of info.

There is a always the classic technique of meeting in a swimming pool or sauna to discuss matters, as it is hard to hide surveillance equipment underneath skimpy clothing, and it does not cope well with water.

Audio surveillance gear is cheaper than video gear, and high resolution video gear able to capture writing on paper without requiring the operator to engage in suspicious behaviour is expensive and may require practice and training. Written, non-verbal techniques have been successfully employed by criminal enterprises during financial bidding to frustrate audio bugs and eavesdropping.

Also consider that your adversaries may employ people skilled at reading lips. Even if you are whispering or talking in hushed tones, it is possible to determine what you are saying. This can also be performed through windows or over great distances using binoculars and telescopes.

Dead Drops (http://en.wikipedia.org/wiki/Dead_drops): A time-honoured bit of espionage tradecraft. With dead drops, stuff is exchanged without either party meeting. To set up a dead drop, two things are required beforehand: an agreed upon signal, and an agreed upon dead drop location.

The signal is best setup in a public place with a lot of pedestrian traffic. Typically a small mark is left on a surface—say, a coloured dot on a subway map where none was before, or certain bit of graffiti in a bathroom stall. When this mark is seen, it means the dead drop has been “activated”—something is waiting for pickup. The “dead drop” could be under a rock in the park, a flower planter in a building, a small hole (well hidden) in a particular movie theatre seat, a crack in a wall etc.

Lots of data can be exchanged—always encrypted, of course!—if small memory cards such as MicroSD (Google Images microSD) units are used. These are about the size of your pinky fingernail. Such a card can be easily hidden in a small hole made in a stuffed theatre chair or a crack in a wall. MicroSD cards have the advantage of being small enough to swallow—a desperate measure to be sure, but one that could prevent information from falling into the hands of your adversaries.

When Police Radio Descriptions

Descriptions of 'Persons Of Interest', when reported over Law Enforcement communications systems, are kept purposefully simple. The more detail included, the more time it takes to confirm and the more likely a mistake will be made.

The articles of clothing paid most attention to are pants and shirts. All the rest are of course paid attention to, especially if they are distinctive or colourful. Pants are much more difficult to remove quickly and inconspicuously in public. People take off shirts and/or change them all the time in public —same for hats and jackets—but how often do people whip off their pants in public? It thusly stands to reason that if you can quickly and inconspicuously change the colour and style of your pants—say from black to white, or pants to shorts—this makes a significant difference. Coupled with a quick shirt change and the loss or addition of a hat, more confusion is sown. A change of shoes is also useful.

Hairstyle is another important descriptive factor. Between the time a description is issued and the the time your adversary goes on the lookout for you, it is very hard for a bald man to suddenly grow hair, a long-haired person to cut their hair or for braids to be unbraided. Avoid distinct hairstyles or colours. The addition or loss of a convincing hair prop (a wig) make a big difference. A less convincing hair prop can be assisted by covering with a hat and letting the lower sections of hair show. It is very handy to employ a toque as such a hat, since the toque can be used as an opaque “bag” to quickly hide the wig in.

Modifications can be made to clothing ahead of time, such as the replacement of key pants seams with thin strips of Velcro so the pants can be quickly ripped off. Or wearing the variety of outdoorsman's pants that come with zippers near the knees so that they may be quickly converted into shorts. Whatever the case, practice pants removal ahead of time with the same shoes you'll be wearing. You MUST be able to get the pants over your shoes, and get them over quickly.

Consider the following simple plan: a white t-shirt under a black long-sleeved shirt, a light pair of shorts under some dark baggy pants, and a hat with some fake long hair built in. A quick strip and you look radically different. As always, you will be served by practicing and role-playing scenarios ahead of time.

Interrogations and Questioning

The are two commonly provided bits of advice when it comes to interrogations: (1) Shut the fuck up and don't say anything; and (2) Nothing you can say to the officers or agents can help.

The first is excellent advice and ought to be strongly heeded. The second is not entirely true—this is how informants can be made.

The TPS has a special department/unit called “Source Control” that deals specifically with the recruitment, creation and placing of informants and their subsequent control and use. Officers from Source Control have, as part of G20 security measures, operated as members of JIG. This is likely a standard form of liaison during such events.

If you are perceived to be part of a targeted group—say, an activist group that the government or police are interested in—you may undergo two rounds of questioning during your interrogation. One, likely the first, will be performed by Source Control officers who will intimidate and regale you with stories of how much trouble you're in, how your life is going to be ruined, jail time etc. They come on fairly heavy and at some point offer you an “out”; a chance to become an informant for considerations at a later date. They may indicate willingness to testify in your favour at trial, saying that you were helpful and provided information and thus deserve leniency in sentencing. They may also tell you that their questions (and your answers) are completely separated and compartmentalized from any subsequent questioning by other “regular” officers. If you agree to inform then you will be provided with a contact number to call upon your bail/release along with promises that meetings will be held secretly and no one will know that you've turned.

The second round of questioning is by “regular” officers and is usually more sedate. The shock of being questioned a second time is typically lesser—you've already been exposed to the techniques. But you will likely be more tired. In either case, interrogation is an uncomfortable, tiring and emotional experience. You will be kept for long periods of time in plain, dingy rooms. Periods of intense questioning will alternate with long periods of silence or isolation that give you time to reflect and think. These are very much part of the plan: they intend to “break” you by alternating between periods of intense stress and isolation. You may have the right to a lawyer in law, but all sorts of deviousness will be employed to keep you from accessing one. They know that speaking to a lawyer is more than just a legal right—it is an emotional connection to another human being during a period of intense stress. The simple act of talking to someone like a lawyer who is on your side and expresses a desire to defend you is a powerful emotional life-preserver, and can destroy an interrogation. Thus it is in your interrogator's interest to delay this connection for as long as possible, by hook or by crook if necessary. They want you alone, isolated, tired and stressed out.

Your best and most immediate defense is to recognize your feelings and emotions for what they are: entirely legitimate responses to purposefully engineered mental torture. You are entitled to feel stressed, you are entitled to feel alone and you are most certainly entitled to feel afraid. Recognizing your emotions gives you some measure of control over them, and this control can be increased by different exercises. One useful one is practicing deep, slow breathing such as in yoga. Stretching regularly helps.

Singing is a time honoured way of persevering through stress. As everyone is unique, methods exist that may work for one person better than for another. Find what works for you.

If you've ever watched interrogations on TV or in movies (and who hasn't!) you might be surprised to realize that many of the techniques are quite real—it can be almost comical. This may in itself be a source of strength to you: interrogations are to a very real extent acting; theatre put on for the purposes of placing you in a scared and stressed mindset. Recognizing your emotions helps you deconstruct the "play" into a series of mere lines being read by actors. Learn to see the comedy in this. Be pleased with yourself for seeing through it.

Some common techniques:

1. Good cop/Bad cop: One cop will be more excitable and in your face, the other, kinder and more relaxed. The "bad cop" will hassle you and then later the "good cop" might take you for a bathroom break, when it will be hoped you'll open up then. Or the "bad cop" will have to leave the room for a sudden phone call, etc. leaving you alone with the "good cop." Alternating between two personalities also serves to keep you off balance.

2. The Big, Thick Folder/File: An officer enters carrying a big, thick folder. They may or may not tell you that it's about you; they're happy to let you make that assumption yourself. During the interrogation they may draw pages from it that are indeed about you...but the rest of the file could very well be filled with blank paper. They want you to think that they have a HUGE amount of information on you. A mental counter to this is to realize that if they really had that much good info on you, they wouldn't need to interrogate you, would they?

3. "Your buddy is in the next room and has told us everything." You may be confident of your ability to withstand an interrogation but most people aren't so confident in their comrades' abilities to withstand one. This technique plays on this natural doubt—everyone rankles at the thought of betrayal. Recognize that your buttons are being pushed. A mental counter to this is to realize that if your comrade really was "spilling the beans", why do they need you to open up and talk as well? They've already got one person talking to them so they don't need someone else—you—to tell them as well.

Officers and agents may make you all sorts of promises or offer to cut you a deal but these mean ABSOUTELY NOTHING and cannot be relied upon. The only personal legally entitled to offer you a deal are Crown Attorneys. If there are no Crown Attorneys in the interrogation room with you, with a document that contains the deal or offer in question, then there's no deal that can be made that is legally binding. Furthermore, you would be a complete fool to take them at their word without your own lawyer present. Remember: police officers and agents are allowed to lie to you, and they do.

Polygraphs (“Lie Detectors”) and Body Language

First off, polygraphs (http://en.wikipedia.org/wiki/Polygraph) —often inaccurately referred to as “lie detectors”—and the evidence obtained from them vary in admissibility from area to area, as well as in the evidentiary “weight” given to them. This is due to something that officers and agents don't want you to know: polygraph machines and their operators are highly inaccurate and the whole process is wildly subjective. They are completely fallible and open to interpretation.

Most important to realize is this: polygraphs DO NOT DETECT LIES! They measure a number of human physiological variables such as pulse rate, breathing and galvanic skin response—moist or sweating palms. These variables roughly correspond to how stressed out you are—this is all that polygraphs measure. They and their operators have no magical insight whatsoever into your mind.

If it's the case that polygraphs measure stress, then if follows that their application during the course of an interrogation—a stressful situation to begin with—can be highly prejudicial. The operator and questioner will attempt to “baseline” out this stress response by asking a series of “control” questions that are designed to elicit verifiable “yes” or “no” answers and reactions—your name, your age, where you live, etc. After a period of such questions they will begin in earnest.

The very process of being questioned is stressful, so even answering truthfully may generate a result that the operator interprets as being misleading or untruthful. Polygraph examinations can be steered into giving whatever results your interrogators desire. Chances are also that the polygraph operator is employed by the same forces interrogating you, so how could they possibly be neutral? You and/or your lawyer are unlikely to be given the option of having the examination conducted by a neutral third-party of your choice.

Even more damning, through study and practice, people can be trained to fool a “lie detector.” And someone such as a sociopath, who is naturally a “cold fish” due to a lack of a conscience and resultant minimalized stress response, can breeze through an examination.

With or without your knowledge, you may also be exposed to someone who is an “expert” in reading body language. Reading body language is far from a science, and is again subject to many of the same criticisms that polygraphs are subject to: are they a neutral third party or are they employed by the forces interrogating you? It is not a cold, clinical mathematical process but one of subjective human interpretation. These “experts” can be misled as well. The same can be said for “experts” in handwriting analysis; it too is a pseudoscience that is highly subjective and one of human interpretation.

All of this is mentioned in order to remove the mystique from these pseudo-scientific processes, and through this realization allow you to reduce your level of fear and raise your strength. Officers or agents may attempt to intimidate you by asking if you'd be willing to take a “lie detector” test. If you have wisely researched the admissibility of polygraph exams in your legal jurisdiction and determined they are inadmissible, state this knowledge and refuse the exam. If the tests are admissible, you should still refuse the exam, but state further to the operator and officers/agents that it is pseudo-scientific,

subjective nonsense— perhaps then they will become prejudiced against you and you may use this as a possible avenue of defense if you are forced into taking an exam.

IN NO CASE AGREE TO A POLYGRAPH EXAM WITHOUT HAVING A LAYWER PRESENT OR WITNESSING THE EXAM. Draw strength from your refusal to submit to their pseudo-scientific, subjective nonsense.

Electronic Physical Tracking and Monitoring

Electronic tracking may be surreptitiously deployed on you for the advantages it offers. As mentioned previously, physical surveillance is a human resource intensive process and may result in gaps or failure. Trained persons may spot or lose people trailing them.

Tracking devices fall into two broad categories: “passive” devices that record location and must be retrieved later in order to download the data, and “active” devices which either continuously, or at intervals, transmit their location. Passive devices may be smaller and consume less energy as they lack a radio unit for providing transmissions—this eats up energy. Nonetheless, both sorts may be small and hard to detect when hidden in or on vehicles.

Two main technologies are employed for determining location in modern tracking devices. The first is, of course, GPS and the second is triangulation via cellular phone radio towers. Both may be employed in order to cover gaps in each other.

Aside from detection and removal of such devices, there are few countermeasures. These devices are fairly cheap and readily available on the Internet and in some stores. It is unlikely such devices will be employed against you but if this is a concern of yours then you ought to avoid the use of vehicles and resort to a combination of walking, public transit or bicycle use.

Some measures to help counter the employment of these devices are to keep your vehicle(s) locked in garages and limit access, and to regularly sweep all exterior surfaces using a mirror-on-a-stick and flashlight. The engine compartment, trunk and vehicle interior ought to be swept as well. Remember: your task is to make your adversary spend as much effort, time and money as possible.

Beware of using OnStar or similarly equipped vehicles for the aforementioned reasons. Avoid using vehicles with automatic toll transponders.

Cell phones, whether you are on foot or in a vehicle need to be turned off and the batteries removed during trips where secrecy and security is required. Cell phones themselves can act as tracking devices as they stay in constant contact with cellular radio towers. Unbeknownst to you, triangulation can be performed to locate you (http://en.wikipedia.org/wiki/Mobile_phone_tracking). Think about it: if you have phone reception, then your phone can find a radio tower. This in turn means that the tower can find YOU. This is one way emergency services can locate people in need of help via their cell phones.

RFID tags (http://en.wikipedia.org/wiki/RFID) are another concern—though their range is limited, they are small and easily hidden in or on many objects. Beware of this—search and be confident of everything you are wearing or carrying on you, in particular ID cards, passports, keys and electronic passes such as proximity cards (http://en.wikipedia.org/wiki/Proximity_cards). Consider purchasing a commercially available RFID scanner to vet items in your possession.

Public Transit, Taxi Concerns and Bicycles

The greatest concern with public transit and taxis is, of course, the presence of cameras. It is not necessarily the case that you can be followed and tracked on video conveniently, the gaps being filled in when a tail loses you in a crowd and you hop on a subway. The most serious concern is that now a record of you exists and at some point in the future it may be dug up and used against you. “Just how long are theses images stored?” is a question you must ask yourself. Given the capacity and low cost of computer storage nowadays, it is quite feasible to archive years of video footage that will be used after the fact to place you in various locations and at times that may be to your detriment. Surveillance cameras do very, very little to prevent anything but they are quite useful in convicting and sentencing people.

Furthermore, buses and taxis contain position reporting technologies so that the companies running them know where they are and can make an economical deployment of them. As a consequence, when you're in a taxi, bus, streetcar or subway you're now in a mobile camera studio that is recording and reporting its location. You may wish to avoid this.

A bicycle is suggested due to its ease of use and portability, and ability to be taken on a sidewalk or used on the road. It's very hard to be hemmed in on a bike compared to a vehicle. Almost anywhere a person can go a bike can go, and a bike can be conveniently disposed of or walked away from without attracting attention or creating a significant financial loss. Bikes are more difficult to add tracking devices to without them being noticed or detected.

Bicycles, in particular mountain bikes, offer other useful opportunities. Many cities and towns have numerous off road bike trails, typically located in forested areas. If a group of activists is equipped with bikes then they can ride into a system of trails where it is much easier to spot people that don't belong or have been following you.

If you get to know your trail system well, then you may be able to use it to evade pursuers or to create secure meeting spots that complicate the surveillance your adversaries may wish to perform on you. Remember, your goal is to force your adversaries to spend as much time, energy and money as possible.

Additionally, the health benefits offered by biking are substantial, and good health is an important component to resisting mental and physical stress. It is easier for a fit, healthy person to escape capture and/or resist interrogation and the experience of being jailed.

Hidden Camera Detection

It is not unheard of for fake look-alike, or disabled, cameras to be placed in order to attract the brunt of attacks and vandalism – or to let people think they're out of view - with hidden cameras placed nearby doing the actual surveillance. So you must consider: am I really, truly seeing all the cameras present?

Hidden cameras themselves can be remarkably small, and when hidden behind a “pinhole” and used with an appropriate lens they are next to impossible to detect via standard physical inspection.

Relatively inexpensive devices, appropriately enough called “camera detectors” (Google Images hidden camera detector) can be purchased from the Internet. These devices use the optical properties of the lenses and sensors to detect cameras, and work whether the camera is on or off. In general appearances these devices look like one-half of a pair of binoculars or small digital camera. You look through the eyepiece as the detector sends out a bright light, which then bounces off the lenses and sensors and back to you, appearing as a spot of brightness. A cheap version of this can be constructed using ultra-bright LEDs placed around the rim of an empty toilet roll, as described in Cory Doctorow's book “Little Brother” ('Little Brother' amazon.com link).

These devices are best suited to darkened interior rooms and do not work so well outside in bright daylight. Still, it is possible to detect hidden cameras outdoors using a system employing a laser that scans over a targeted area coupled to a visual receiver, which picks up the reflections. This is a more expensive and less practical solution that will likely not be available to you.

Telephone Tapping/Interception

Unless you are the target of amateurish phone tapping, you will never know if your cell phone or land-line is being tapped. All modern telephone communications are carried over digital networks at one point or another.

Adversaries from government agencies can, via the telecommunications providers' equipment and facilities, simply copy the contents of your calls in digital form remotely, and even in real time. There is no need to physically access your telephones or premises to perform this. You will *not* hear mysterious clicks or pops, echoes, or suffer an increase in dropped calls (if you do, then it is an amateur tap, perhaps by a private investigator or the media). It is silent and undetectable.

Calls that are transmitted at one point or another over satellite are also subject to undetectable eavesdropping.

DO NOT RELY ON ANY SORT OF TELEPHONE for the communication or dissemination of secret or sensitive information.

http://en.wikipedia.org/wiki/Phone_tapping

Jail Etiquette

At some point you may find yourself in jail—for whatever reason—right or wrong. Knowing some basic rules and etiquette will help reduce your stress and keep you safer.

First off, every institution has its own variation on rules and its own schedules. In some you may be out of your cell from morning to evening, others you will be out for two hours, then back in your cell for two hours for a meal, then out and back in again for each meal until evening lockup. You will need to be adaptable.

Above all: be polite! Be a quiet, respectful person. Ask before doing or using anything. Canada is a generally polite nation and this even extends into jail—this is not like “Oz” from TV (http://en.wikipedia.org/wiki/Oz_(TV_series)).

Some people are more sensitive to etiquette issues than others. For instance, some people may have a favourite seat or bench—so do yourself a favour and ask before sitting down, for example. Sometimes people are just in a very bad mood, or got bad news, and strike out at the slightest annoyance. Don't be annoying.

Generally speaking, people who don't go looking for trouble won't find it. Violence does happen, yes, but very rarely for no reason—if you keep yourself aware of your environment you will be able to see it coming.

The following rules will serve you well regardless of what institution you wind up in.

1. Don't touch or move other people's stuff. If you absolutely have to, ASK FIRST.

2. No whistling! Seriously. This is an old tradition—birds whistle because they are free, and so only two sorts of people can whistle—those who are free, and those on their way to their own execution (at least historically), since they will be “free” shortly. Whistling shows disrespect for those (historically) condemned to death or already executed. As I said, it's an old tradition.

3. Shower when you come back from court.

4. Don't wear your shoes in the shower; leave them outside the shower stall.

5. Change in the shower stall—never show boxers outside the shower or outside your cell.

6. Never clean the phone handset with your towel—it's touched your private areas and people don't want that near their face.

7. Never flush the toilet after “lights out” and before “lights up.” If you must use the bathroom after 'lights out', cover the toilet bowl with a shirt or towel to reduce the smell.

8. Cover your mouth and nose with your shirt or elbow when you cough or sneeze.

9. Don't look in other people's cells—it's like looking in someone else's house. Don't enter someone else's cell, even if they're inside, without asking permission first.

10. Clean up after yourself.

11. Don't spit in the sink. Spit in the toilet if you're brushing your teeth.

12. Flush the toilet constantly when using it—no one wants to smell excrement.

13. If you need something, talk to the “servers” or senior people on your range. Avoid talking to the “COs” [Correctional Officers]

14. Do NOT, under ANY circumstance “rat” on other inmates! Once you are known as a rat, you life will be hell and you will be subject to violence.

15. Never call anyone a “goof.” It sounds innocuous, but the word “goof” has an *entirely* different meaning in prison and is probably the WORST insults you can use.

16. Don't “PC up” (PC = Protective Custody) or “go to the glass” (this means using the intercom to call a CO and ask to be taken off the range). PC is where rapists and child molesters go and you *cannot* risk being tainted as such. Child molesters and rapists are HATED and subject to frequent violence. If you want to “PC up” because you've been assaulted, DON'T. Suck it up and stay where you are. You will be respected for not calling a CO and for not running away. Is this messed up? Perhaps, but this is Jail, not regular society.

17. There is usually a queue for phones and showers. If no one is on the phone or in the shower, ask anyway. Sometimes—fair or not—certain phones or showers are reserved for certain people or groups.

18. Racism is not well tolerated. Respect people of all races equally. Some people may joke with each other in ways that appear to violate this, but they have a relationship with each other that permits this. You don't, so don't try it.

19. Don't cheat or scam another inmate, EVER. Avoid borrowing or getting in debt, but if you do, make sure you understand the terms of the deal before agreeing. Pay people back on time—*always* honour your word.

20. Don't leave soap in the shower—or anything else.

21. Wash your hands after using the bathroom.

22. “Do your own time”: no one needs the additional burden of hearing your sad story—jail is a miserable enough place to be. It's hard, but keep your problems to yourself. At least until you've established some friends who are willing to put up with it.

Some further advice: do not get involved in buying or selling drugs or tobacco in jail. It is expensive—*far* more so than the street—and when money is involved, problems often ensue when people do not pay on time or get too far in debt. Furthermore, there is always the risk of being robbed or becoming addicted. Stay clean, and do not borrow or lend money, or help people move money around on the outside.

Further Thoughts on Secure File Deletion, and Verification of Secure Deletion

I am starting this section under the assumption that you are using the Linux operating system because that is what I use most often and am most familiar with. Additional operating systems, such as OSX (Mac) and Windows will be addressed later.

The advantage to using Linux is that it is *free;* both from a price and an intellectual property perspective. You have an incredible variety of excellent free tools to use that work extremely well. Contrast this to OSX, and especially Windows, where you will likely have to pay money (although to be fair, plenty of shareware and freeware exists for both Windows and OSX). Additionally, many of the people who build and maintain Linux (and the different the flavours of Linux referred to as 'distributions' http://en.wikipedia.org/wiki/Linux_distribution) are strongly pro-freedom and often have politics compatible with those in the activist community. I would strongly advocate supporting them, and Linux, if for no other reason than this.

Another advantage to using free, easily downloadable software tools and Linux is that there is no registration needed. This means there is less information out there that can be tied back to you. For instance, if you were to install Windows XP on an Eeepc and then left it behind when you made a quick escape, a Law Enforcement agency now has your machine in their possession. Now an OS serial/registration number can potentially be tied back to you. The same goes for any registered software present on the machine. Would you write your name and address on the same computer? No. Of course, if your software is pirated, then this is likely not an issue.

The tool I use most frequently to securely delete files is called “shred”. If you are running a modern distribution of Linux, then it's quite probably already installed. More info can be located at the following URL: http://en.wikipedia.org/wiki/Shred_(Unix).

The tool I use most frequently to verify that data has been securely deleted is called 'PhotoRec' and is located at the following URL: http://www.cgsecurity.org/wiki/PhotoRec

The following is taken from PhotoRec's web page: *PhotoRec is file data recovery software designed to recover lost files including video, documents and archives from hard disks, CD-ROMs, and lost pictures (thus the Photo Recovery name) from digital camera memory. PhotoRec ignores the file system and goes after the underlying data, so it will still work even if your media's file system has been severely damaged or reformatted.*

The reason PhotoRec works so well requires some understanding of what actually happens when you 'delete' a file on your computer. The fact of the matter is that the file is *not actually removed,* but for lack of a better word, is dereferenced.

A simple analogy can explain this better. Consider a school notebook full of text. You decide you want to delete the section you titled “Study notes for quiz #3” since you passed the quiz last week and don't need that information anymore. You want to re-use that paper for other, more relevant notes, such as for quiz #4 which is next month.

What you do is to grab your eraser and rub-out “Study notes for quiz #3” at the top of the page. That's it - you don't actually erase any of the notes! Now if you flip through your note book, there's nothing that tells you “Here's where the study notes for quiz #3 are”.

But, wait a second! All the pages are still there, with your writing on them. You can still read them. In short, all you've done is removed the *reference* to the study notes. You don't actually rub out any of your writing until the very moment you decide to re-use the paper.

This is an admittedly lame example, but it's quite in line with what happens when you delete a file on your computer. The contents are still there, and will be for some time, until your computer happens to need some free space and writes over the section where the file used to be. This can take a surprising amount of time – perhaps even years for someone who has a very large hard drive and doesn't do a whole lot with their computer.

Don't forget about 'data remanence': http://en.wikipedia.org/wiki/Data_remanence.

PhotoRec, and other forensic analysis tools, operate by ignoring the 'table of contents' and scanning the entire device, looking for structure. When it sees structure, then it knows something is there and attempts to reconstruct it.

You must never, ever rely on deletion tools, even secure deletion tools, without verifying how well they work. You must practice creating files, deleting or shredding them, and then running recovery tools such as PhotoRec to verify that either no data is recovered, or that the recovered data is full of garbage. The Shred tool, for instance, overwrites the file multiple times with special patterns of data before it deletes the file. This way, if the file is recovered, it's still useless to your adversaries as it contains useless garbage.

It is recommended that if security is a concern, do not reuse USB or memory cards. Once their use has been served, physically destroy them. Take the shells off if possible, crush the circuit boards, and fracture the chips into multiple pieces. Then you may wish to take these pieces and expose them to extremely strong heat. It is recommended to use micro-SD cards due to their small, thin nature – these can be successfully shredded using machines that are capable of shredding CDs or DVDs – you do have one of these shredders, right? To ensure the microSD card passes through the shredder properly, it is helpful to tape it to a piece of paper and pass it through multiple times, verifying afterwards that the microSD card has been mauled into several pieces.

Computer Forensic Software and Procedures Used by Law Enforcement

The computer forensic software packages most commonly used by Law Enforcement are called EnCase (http://en.wikipedia.org/wiki/Encase, http://www.guidancesoftware.com/) and Access Data FTK (http://en.wikipedia.org/wiki/FTK, http://accessdata.com/products/computer-forensics/ftk). These packages typically cost several thousand dollars, although you may find older pirated versions floating around the Internet.

These packages are almost always used in conjunction with a piece of hardware called a 'write blocker' (http://en.wikipedia.org/wiki/Write_blocker). Write blockers are used to ensure that during the process of 'imaging' a drive (http://en.wikipedia.org/wiki/Disk_image) the contents are not modified or changed in any way, and so remain forensically valid and admissible in court. If there was any possibility that during the process used by Law Enforcement time stamps or even content was changed or damaged, then the Defense has grounds to contest the validity of the evidence which may lead to its exclusion. The original hard drive is never used after imaging, and all forensic work is done on the drive image. Write blockers cost anywhere from a few hundred dollars to several thousand.

The typical procedure performed when Law Enforcement encounters a computer they wish to analyze is to shut the machine down, extract the hard drive, install a write blocker, and use a piece of software to make an image of the drive. This drive image is then examined with a program like EnCase or FTK, which analyzes, catalogs and reports on the contents of the drive. The EnCase or FTK report (which usually contains everything on the hard drive) typically constitutes a part of the disclosure provided to defendants.

This is why FDE (Full Disk Encryption http://en.wikipedia.org/wiki/FDE#Full_disk_encryption) support present in many hard drives and computers is highly valuable (for an example, refer to http://www.thinkwiki.org/wiki/Full_Disk_Encryption_(FDE)). With FDE present and engaged on a drive, there is nothing that EnCase or FTK can do. When a drive using FDE is extracted from a computer and imaged for analysis, the entire contents are rendered useless for forensic analysis.

However, FDE is subject to something referred to as the 'cold boot' attack: http://en.wikipedia.org/wiki/Cold_boot_attack.

From the article: *In cryptography, a cold boot attack (or to a lesser extent, a platform reset attack) is a type of side channel attack in which an attacker with physical access to a computer is able to retrieve encryption keys from a running operating system after using a cold reboot to restart the machine from a completely "off" state. The attack relies on the data remanence property of DRAM and SRAM* [NB: two types of computer memory] *to retrieve memory contents which remain readable in the* ***seconds to minutes*** *after power has been removed.*

While rather unlikely that this attack vector will be used against you, given that it must be performed within seconds or minutes (or longer periods of time if the components are cooled with low temperature substances such as freon, chilled carbon dioxide, or liquid nitrogen), much less whether they'll successfully pull it off, it is something to be aware of. Videos are available on YouTube at the

time of this writing that demonstrate how a 'cold boot' attack is performed. This is why you still need to encrypt your sensitive data even if you have FDE enabled. Remember to adhere to the principle of defense in depth (http://en.wikipedia.org/wiki/Defense_in_depth) and use multiple levels of encryption.

Facial and Gait Recognition Technology (Biometrics)

It ought to be well known that Law Enforcement agents are regularly (one should assume *always*) present at demonstrations, protests and 'riots' videotaping the individuals present. This is not only done to gather evidence of the activities but also to capture people on tape so they can identify individuals later using facial recognition software (http://en.wikipedia.org/wiki/Facial_recognition_system).

Some of the software is hit-or-miss, and seldom provides a perfect match but rather more along the lines of a percentage match, but it is valid and can indeed be used to identify people. However, in order for it to be of any use, they need to have a baseline – an existing picture of your face – already in their possession ***or*** to obtain a picture of you in the future. Clearly, this means that if you don't wish to be identified during an activity that may be perceived by Law Enforcement as troublesome or illegal (however legitimate it is or that you feel it to be) you must take steps to disguise yourself during said activities.

For a match to be performed using the software, the highest quality photo possible is desired. The larger the area of your face they have on film, the better the match will be. A full frontal shot is preferred, but matches based on oblique photos (shots taken at an angle) can still be used.

It is effectively impossible for an individual to change the physical structure of their face. The distance between the eyes, the position of the nose relative to the eyes and mouth and ears, the chin, the forehead (and likewise)... none of these change. Steps such as changing the colour of your eyes using contact lenses, packing cotton between your gums and your lips, or prosthetic noses make no effective difference, nor does facial hair. Standard plastic surgery has minimal impact as it only changes the layers of skin and fat, and does not alter the underlying bone structure.

If all they have are photos of people wearing bandannas such that only the eyes are exposed, this can still be used to eliminate individuals from a pool of suspects. Thus it follows that if you want to eliminate the possibility of being compromised due to a facial recognition match, you need to obscure your entire head and cover your eyes. The problem with this is that there is law in the Canadian Criminal Code that make it an offense to wear a 'disguise' with the intent to commit an indictable offense (Disguise With Intent - Criminal Code - R.S.C., 1985, c. C-46 (Section 351)). At the very least, wearing a disguise will be used against you in court as evidence that you knew what you were doing or planning was wrong or illegal. There are also plans afoot to make the wearing of a disguise during a peaceable assembly (or what they will all of a sudden, at their convenience, call “Riots and Unlawful Assemblies”) a crime (Bill C-309).

Don't fool yourself into thinking that legitimate democratic protest will necessarily stop them from using the situation as an excuse to falsely accuse you of committing an offense, forcing you to remove your disguise at some point in order to photograph you. They may very well opt to do just that (if they haven't regularly done so already), leaving you to endure the process of criminal justice just to wind up clearing yourself later.

It is not unreasonable at all to think that they will target masked/disguised individuals specifically for the purposes of unmasking and photographing them and then cataloging them for future use. They have

already done so on multiple occasions, afterwards circulating this information to agencies in different jurisdictions and countries. Law Enforcement is all about collecting data for future use without necessarily intending to use it in service of the immediate goal or situation at hand. This is part of the reason that when you obtain a passport, the government employees are very particular about you standing still and not smiling (smiling throws off the biometrics!). If you have a passport, you are already in a catalog that can be, and has been, shared among multiple agencies and countries for the purposes of denying you entry or arresting you later – especially the USA and their DHS.

This may cause a problem for the community when people, even participants of the actions themselves, take videos or photographs. The same applies to media, television stations, nearby businesses with security cameras (as well as the cameras present in almost all ATMs), and even curious tourists. Law Enforcement agencies can, and have, subpoenaed or outright illegally confiscated images, video and media in order to further the cataloging and prosecution of individuals.

So, what are we to do? We can't very well ban all cameras from actions – that is against our own best interests and the interests of the public. It is also impossible, given that cameras can be hidden everywhere and are (given the current state of technology) effectively impossible to detect if someone takes fairly easy measures to conceal them.

There are no easy answers to this question. All that can be confidently said is that if you are engaging in an activity which may prove troublesome to you later on, you are advised to cover your entire head and wear sunglasses.

There are other methods of identifying you using biometrics. A more recent innovation is referred to as 'gait analysis' (http://en.wikipedia.org/wiki/Gait_analysis#Biometric_identification_and_forensics), your 'gait' being the way you walk.

From the article: *Minor variations in gait style can be used as a biometric identifier to identify individual people. The parameters are grouped to spatial-temporal (step length, step width, walking speed, cycle time) and kinematic (joint rotation of the hip, knee and ankle, mean joint angles of the hip/knee/ankle, and thigh/trunk/foot angles) classes. There is a high correlation between step length and height of a person.*

One anecdotal method of throwing off gait analysis involves placing a small stone or object in your shoe(s), which will cause you to walk differently due to the discomfort you encounter. This is referred to in Corey Doctorow's book excellent book, Little Brother ('Little Brother' amazon.com link). It stands to reason that gait analysis would also be thrown off by anything that affects your mobility, such as wearing a cast, or anything that restricts the movement of your feet, legs and waist.

Avoiding Fingerprints

Everyone knows about fingerprints.

However, many people are not aware that latex gloves are ***not*** a good method of preventing fingerprints from being left behind. Thin latex gloves (such as those used by doctors or surgeons) are designed only to prevent the transmission of body fluids and contaminants without significantly affecting the ability of the user to feel what they are doing (think about the design of condoms!). With a pair of latex gloves on it is entirely possible to leave a fingerprint behind – this has, in fact, led to the identification and conviction of individuals in the past. You should always assume that thin gloves made of different materials, such as vinyl, are subject to the same problem.

For this reason, if you wish to avoiding leaving fingerprints behind, you must test the gloves to see how they perform.

Put on a pair of gloves, and using your thumb and several fingertips (on both hands) rub them gently on your face or forehead (the face and forehead are among the oiliest parts of the human body) so that they pick up a little grease and oil. Alternately you may choose to use artificial oils to simulate this.

Then place your thumb and fingertips against a flat sheet of glass or other smooth surface in an attempt to leave a print behind – handle this surface as you would normally, that is to say, using regular amounts of pressure.

Now examine the surface, perhaps using a magnifying glass and/or tilting the surface at an angle so it catches the light better, and examine the prints left behind. Afterwards it is also advised to lightly dust this surface with some sort of powder (such as graphite, which is what the 'lead' in pencils is actually made of) to make the prints stand out. This is the same sort of thing that Law Enforcement agents do when dusting for fingerprints. In short, you are advised to duplicate the same sort of procedures Law Enforcement uses in order to test the effectiveness of your gloves.

Continue with this process, testing different varieties of gloves and different combinations of layers, until you have confirmed a glove configuration that leaves no fingerprints behind. Additionally, you may wish to use an ink-pad (Google Images inkpad link) and a piece of glossy white paper in an attempt to print yourself.

One glove type that is inexpensive and easy to dispose of are the cotton variety available at many pharmacies and drug stores (Google Images dermatological cotton gloves link). These gloves are used by people who have allergies to latex or other plastics, among other uses (such as handling sensitive optics and lenses for cameras, and keeping electronic components contamination free). They have the added advantage of burning fairly well down to ashes. Be aware, however, that cotton gloves have less grip than either latex or vinyl.

In a pinch, dish gloves (Google Images dish gloves link) can be used, but they are harder to dispose of quickly by burning due to the amount of material they contain. Their thickness and the common presence of textured fingertips make them unlikely to leave any usable fingerprint behind, but you must

still confirm this to ensure your safety. Furthermore, given their rather robust construction, it is possible that *the gloves themselves* can be printed due to wear marks or damage, much like identifying shoe prints.

All gloves must be disposed of carefully after use – ***do not*** simply throw them away as it is trivial to obtain fingerprints from the inside of latex or vinyl gloves. Burn the gloves, or dissolve them in solvent, so nothing remains that a fingerprint can be lifted from.

All objects to be used, or disposed of afterwards, must undergo a thorough wipe down. It is advised to use a rubbing alcohol (as high a percentage alcohol as possible) or ammonia based cleaning solution, as both ammonia and alcohol are good at dissolving the grease/oils composing composing fingerprints. Do not think that you can simply throw the objects in the lake or a river, as prints have successfully been lifted from submerged objects in the past, though of course it makes the process much harder for Law Enforcement.

All removable pieces must be removed and wiped down, as well as any sockets or bays they were removed from. If you've opened up an object to work on it, then the interior of it must be wiped down as well (no use wiping down the case if they wind up lifting a fingerprint off that new memory or hard drive you installed last year).

For this reason, any object or computer to be used in a sensitive action is best obtained for that purpose (and that purpose alone) and kept in its box or wrapping until the moment it is needed. It ought to be handled wearing gloves for the entire lifetime of its use, and disposed of immediately and irreversibly once its use has been served. It is highly aggravating and requires a significant amount of work to 'wipe down' any complex object in order to render it forensically useless if it has been in use for any amount of time.

Thoughts on Informants and Infiltrators

This is an unpleasant topic but it requires serious thought. It is *strongly* suggested that you read the following links and become familiar with the practices they recommend and information they contain: http://security.resist.ca/personal/culture.shtml, and http://security.resist.ca/personal/securityzine3.pdf.

The fact of the matter is that informants (AKA rats and snitches) and infiltrators (people spying on a group on behalf of Law Enforcement or other organizations) are a fact of life. They have always existed, they always will, and there is little or nothing you can do about it. You must simply accept it as a fact of life and move on. It's the price of admission.

If you expend too much effort trying to determine who is an informant or infiltrator, then you have less time to spend on the really important matters. Furthermore, Law Enforcement is well served when a group becomes suspicious and paranoid, excessively investigating and analyzing their own people.

Without spending any government money or resources a group begins compromising its ability to work effectively and then begins to destroy itself from the inside. This serves their purpose admirably. Why send an agent in to disrupt and divide a group, costing time, money and potentially the safety of the agent when you can simply plant a rumour and let the group do all the work themselves? Sowing dissension among the ranks is one of their key techniques.

When a group becomes suspicious of its people it is damaging in other ways. It becomes harder to attract new people into the group when current members are mistrustful of new faces. Movements and organizations thrive, indeed require, an influx of new people in order to expand and accomplish their goal (in most cases, at least). So even the hint, a rumour, of informers and infiltrators can serve to cut off the lifeblood of a group.

My advice is to welcome everyone with open arms, and to ask very few questions. Matters of personnel security can only be sorted out with time and experience.

Nonetheless there are steps you can take, most of which are common sense:

1. Actions that may be perceived as troublesome or illegal by Law Enforcement (other than mass protest, of course) are to be restricted to the smallest group necessary and among individuals with a well established trust and some history together.

2. Any actions that may be perceived by Law Enforcement as troublesome or illegal are *never* to be talked about to people outside this small core group. No individual is to *ever* talk, especially brag, about being involved in such actions, in the past or in other organizations. But keep in mind that just because someone asks about becoming involved in such an action does not necessarily mean they are an informer or infiltrator – they may simply be excited and strongly desire to accomplish something they perceive as meaningful.

3. Any individual asking about past actions, who was involved in them, and who may be involved in upcoming actions is to be confronted with a *polite* refusal to disclose anything at all. You will neither confirm nor deny *anything* to them. It is very important that after such a confrontation you then *politely* explain to them that asking for such information is a violation of common sense, a violation of the group's security culture (http://en.wikipedia.org/wiki/Security_culture), and an all around bad idea that will not serve them well and will compromise their future ability to act meaningfully. You very much want to avoid making people feel embarrassed, angry, or useless. Consider it your job to help breed as many high quality activists as possible – you don't accomplish this by pissing people off, or making them feel like idiots, and scaring them away.

4. People with conditions, such as drug addiction, are often weak points when it comes to interrogation and criminal justice procedures. It is also a convenient vector to pressure a person into turning informant when they can be confronted with the possibility of time in jail that would threaten their relationship/marriage or welfare of their children. This is not to say that married people or people with children ought not to be involved in actions, but rather that they must carefully take stock of the potential trouble they might wind up in. It's a well worn cliché: ***If you can't do the time, don't do the crime***. When you are up against the government and Law Enforcement, you must accept that it is entirely possible, even likely, you will be arrested, subject to assault, spend time in jail, and exhaust a large part (or all) of your life savings defending yourself.

5. People who regularly spread rumours (that is to say, guesses and/or wild speculation unbacked by legitimate and/or verifiable evidence) about the presence of informants or infiltrators, *especially* when they frequently talk to many people about a specific person or group of people as being informants or infiltrators are to be *politely* confronted and asked to stop.
It's also old news: put quite frankly, only an idiot would assume that this is something new. You must then explain to them why their rumour spreading is both distasteful and dangerous. As soon as people begin spreading rumours about informants or infiltrators they begin, whether they know it or not, to serve the purposes of the government and Law Enforcement. One of the worst things a person can do is to gossip and spread rumours. These sorts of people may prove to be more damaging to a movement than the actual informer or infiltrator themselves. In no way, however, should this advice be interpreted as advising people to keep legitimate concerns to themselves and not to share. There is a fine line being expressing legitimate concern and rumour mongering.

But it must be said: how committed are you *really* to a cause if you are not willing to sacrifice your freedom in service of your beliefs? This is not a game and this is no place for the weekend warrior or poseur who thinks it's cool and fashionable to participate in a protest, or does something because it's what all their friends are doing. This is war, and the dividends of war are too often misery and death.