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

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

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

– The Anti-Terrorist

Introduction

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

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

Defensive computing holds better promise for securing your records than any legal remedies. Undertaking the responsibility upon yourself alone for securing your archived records quickly becomes much more of a pragmatic question, which appears to be one that quite a number of people would rather just avoid. Whether it be due to computer illiteracy or moral cowardice, technological innovations for both digital and paper records are routinely ignored by not only disingenuous activists, but also by their incompetent followers alike.

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

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

PART I

Constitutionality & Case Law of Fourth Amendment "Papers"

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

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

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

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

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

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

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

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

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

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

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

1. Records and documents which reflect the sale, trade, pawn, receipt, or disposition of any firearm, ammunition, and/or firearm components and accessories, buyer lists, seller lists, books reflecting the value of firearms or ammunition, and notes (cryptic or otherwise), pay-owe sheets, records of sales, log books, ledgers, documents, shipping records and indicia, materials used to package firearms and ammunition for shipment, and photographs which reflect relationships between unidentified co-conspirators to include personal telephone/address books, electronic organizers, and rolodexes.

1. Records that establish the person who have control, possession, custody, or dominion over the property and vehicles searched and from which evidence is seized, such as: personal mail, checkbooks, personal identification, notes, other correspondence, utility bills, rent receipts, payment receipts, financial documents, keys, photographs (developed or undeveloped), leases, mortgage bills, vehicle registration information or ownership warranties, receipts for vehicle parts of repairs, telephone answering machine introductions, and fingerprints.

1. Documents and manuals that depict or instruct on subjects such as firearms conversion kits or parts, automatic weapons concealment, smuggling, or state and federal firearm and ammunition laws.

1. Safes, strong boxes, and/or other secure receptacles for the maintenance of valuable items, firearms and/or documents including books, records, and any keys or other evidence of the existence and use of any lockers, safety deposit boxes or other secure receptacles located elsewhere than at the premises.

1. Computers, to include all electronic data stored in the computer such as photos, documents, notes, correspondence, firearms records, financial records, names, addresses, telephone numbers, and other records relating to the acquisition, purchase, transfer, possession, manufacturing and/or disposition of firearms.

1. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items:

- a) Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;
- b) Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;
- c) Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMS, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;
- d) Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;
- e) Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Apparently, a **private membership organic food-buying co-op** is considered by the Ohio judiciary to be a "retail food establishment" subject to licensure, just because they said so; as such, this is the Ohio government's primary justification for the police raid on Manna Storehouse. I seriously doubt Chad Stowers, one of John and Jacqueline's adult children, reenlisted in the U.S. Navy for another tour in Iraq once he heard of what happened to his parents and siblings, don't you think?

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

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

END PART I

PART II

Digital & Paper File Hardening

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

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

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

You should consider taking a rather "minimalist" approach to sorting your paperwork. What you learn from sorting your paper records can transfer over to doing so with your digital ones without too much of a fuss over adaptation. Although *how* to organize your paper records can be individuated , I think the core idea here is to reassess your priorities, and by doing so, you can more easily strip away all that excess baggage that fails to bring value into your life. Emotionally letting go of sentimentality, whether that be taking the Giant Leap or through Baby Steps, is integral towards getting your paper records under control by reducing your overall level of clutter.

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

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

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

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

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

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

User error is a fear that, while justifiable in particular circumstances, is frequently exaggerated due to other mitigating factors, such as software infections or hardware breakdowns. The main reason people don't use encryption or locks is that they are primarily concerned *not* with having their information being stolen or otherwise used against them, but rather, having their access to such information being blocked, mainly due to forgetting their passwords or misplacing their keys. Two methods that could be used to overcome these fears is to use a password manager program (software application) and a laptop lock whose key is kept on a compact key holder (hardware solution).

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

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

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

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

A Layman's Tutorial on Performing Secured Record Archival

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

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

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

Scan involves not just antivirus and anti-malware programs, but also the digitization of paper records. **Inventory** determines just how much and what kind of records there actually are, with the goal of being able to reduce the extraneous clutter, whether in your filing cabinet or on your hard drive. **Backup** spreads out all the organized records amongst dissimilar storage media, so that in the event one of them fails or is otherwise inaccessible, your data can still be accessed via an identical copy. **Encrypt** is a layer of actual security, although this is mostly applicable to digital records only. **Cache** is the other layer of security that applies equally to both digital and paper records through the use of physical hideaways.

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

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

141129 – hard drive archival status.jpg

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

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

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

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

- Michael Conner's *How to Hide Anything*
- Jack Luger's *The Big Book of Secret Hiding Places*
- Dennis Fiery's *How to Hide Things in Public Places*

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

END PART II

Conclusion: Observations on Strategic Implications

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

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

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

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

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

Passively assuming that digital encryption programs have a viable efficacy based solely on faith alone is not good enough anymore – **Americans need proof that they work**. For my own initial wishlist, I'd like to know what security audits would potentially reveal about KeePassX, GPGTools, and Safe. Although I understand that security audits can be quite costly, as was the case with SpiderOak's Crypton project, yet, if over 116,000 people donated $6,675,039 in 17 days because of the recent Orlando nightclub shooting, then why can't a cheaper bill be footed so that fewer individuals find themselves becoming political prisoners on the mere accusation of having committed a victimless crime?

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

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