The PARANOID Newsletter

Because they ARE out to get you.

A good walker leaves no tracks;
A good speaker makes no slips;
A good reckoner needs no tally.
A good door needs no lock,
Yet no one can open it.
This is called "following the light.
-Tao Te Ching

Introduction

This is the tenth issue of the PARANOID newsletter. This newsletter is for the person who takes their privacy VERY seriously. Lets face it, America is a POLICE STATE. Anything the government doesn't like is now considered terrorism. What would our founding fathers say if they were alive today!

Principles of pick gun forensics

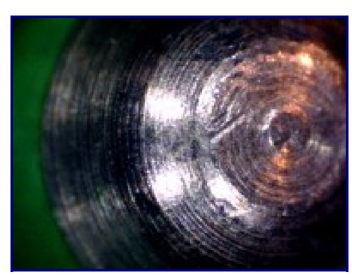
Manual pick guns are spring-loaded tools that resemble a toy gun with a lockpick attached to the front. The lockpick is interchangeable, and referred to as the "needle." To open the lock, the needle is inserted in the lock and placed under all pin stacks. As with lockpicking, a separate tension tool is used to apply tension and rotate the plug. Light tension is applied to the tension tool and the trigger of the pick gun is fired. According to physics, the kinetic energy transfers from bottom pin to top pin, causing the top pins to "jump" in their chambers. If all top pins jump above the shear-line at the same time, the plug can be rotated to unlock the lock.

Electric and vibrational pick guns work on a similar principle, but instead oscillate the needle back and forth, causing it to vibrate. The tool is controlled to get the resonating frequency of the needle at the right point so that top pins jump above the shear-line.

The main source of forensic evidence with pick guns is on the bottom of the pins, where the needle strikes. We may also see marks in the plug if the needle is not properly positioned and makes contact with the plug walls when triggered. The cam on the back of the lock may also have marks if the needle is inserted too far into the lock. As is the case with lockpicking, we can also identify tool marks left by the tension tool.

In the case of vibrational or electric pick guns, we will see considerably more evidence on the plug walls because the device is constantly moving.

The striking of the pick gun needle against the bottom pins causes very clear forensic evidence. Unlike picking, which causes scratches, the pick gun causes impact marks that, when done many times, begin to resemble the spokes of a bicycle along the circumference of the pin.

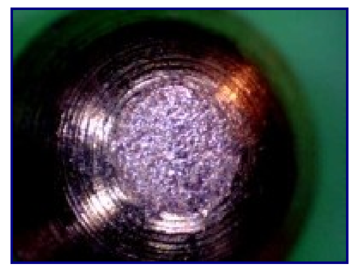


The marks left by a pick gun are so distinct, compared to the rest of the pin, that is is often possible to count them to determine how many times the pick gun was triggered. Each time the needle strikes, the bottom pins may rotate slightly, allowing marks to be separate and distinct.

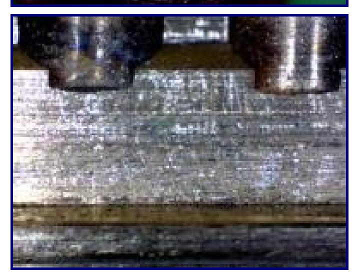
As with many other techniques, the cam of the lock is a good source of forensic evidence. This is sometimes the best evidence, because the needle of pick gun often shears very clear marks into the cam. In this case, the pick gun appears to have been used at least eight times.

Up close we can see the very distinct markings left on the cam by the pick gun needle. These marks are well defined and would make for a very good tool mark comparison. Because they are so deep, the pick gun needle may also have material residue that can be linked back to this cam.

Electric and vibrational pick guns leave different marks because they are constantly moving in the lock. When using this type of pick gun, material removal from the components and plug is so extreme that you can see brass particles exiting the keyway. In this photo, repeated use of a vibration pick gives the bottom pins a rough, uneven texture.



Constant movement of the vibrational pick gun needle causes numerous tool marks on the plug walls, as well. In this photo, various vertical scratches are present throughout the length of the plug. Some vibration picks also leave a stuttered or angled type of tool mark on the plug walls.



Principles of key bumping forensics

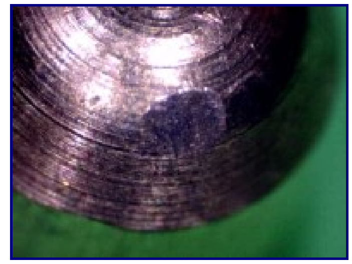
To bump a lock, a key is acquired that fits the keyway of the lock. The key is modified so that all cuts are at their lowest depths or lower. This is commonly referred to as a "999 key," because 9 is usually the designated lowest cut depth. If done by hand, a key gauge or micrometer can be used to measure the key and ensure cuts are deep enough. If done with a key machine, the key may be duplicated from a working bump key, or cut by code to the lowest depths.

In the pull-out method, the key is inserted into the lock fully then withdrawn one pin space. In the minimal movement method, the key is further modified by removing material from the tip and shoulder of the key. The minimal-movement key is inserted completely into the lock. In both cases, light tension is applied to the key and a tool (known as a bump hammer) is used to impact the bow of the key, causing the key to be forced into the lock.

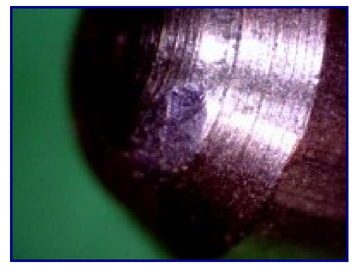
The impact on the key causes kinetic energy to travel from the key to the top pins, causing the top pins to momentarily jump. If all top pins jump above the shear-line while tension is applied the plug is free to rotate.

As with pick guns, the main source of forensic evidence of bumping is on the pins themselves. The action of striking the bump key into the lock causes distinct dents and scratches on the bottom pins. Bumping also affects the face of the plug, the keyway profile, pin chambers, top pins, and the bump key itself.

Forensic Evidence



The act of key bumping basically slams the key against the bottom pins to allow for kinetic energy to be transferred from the key to the top pins. Because they are immobile and absorb the kinetic energy, this causes considerable damage to the bottom pins in the form of large dents and scratches.



A bump key that is cut by hand, with a low speed key cutter, or made of a considerably stronger material (steel, iron, nickel-silver) than the pins may act as a file as it impacts bottom pins. In this photo, light scratches can be seen traveling through the bumping dent.

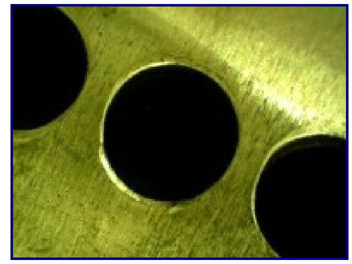
Alternate lighting may be used to illuminate bumping scratches and dents more efficiently. In this photo, there are dents on the left, center, and top of the pin, as well as scratches. In many cases it is posisble to count the number of times the bump key was used by counting the dents.

Bumping is rarely 100% successful, either because bottom pins are bumped above shear line, or top pins are not bumped high enough. When this happens the tension applied will misfire, causing one or more top pins to bind. This causes light shearing against the bottom of the top pins.

Some top pin designs will be more affected by bumping than others. In this photo, a spool pin with serrated edges is shown. Repeated bumping of this pin has caused the serration to close up (compare with previous photo). In general, situations like this slightly decrease pick resistance.

In some pin designs the bottoms of the top pins will be considerably damaged by bumping. In this case, the bottom pins are lightly rounded on both sides, allowing them to be inserted either way. When bumped repeatedly, the bottoms of the top pin become considerably dented.

The pin chambers within the plug may also be damaged by bumping. When kinetic energy does not properly transfer to the top pin, the pin stack may instead press against the chamber walls (caused by the movement of the bump key). Repeated bumping may cause these areas to distort, stretching in various directions.



One of the most noticeable pieces of evidence from key bumping is damage to the face of the lock. This is caused by the shoulder of the key impacting the area above and below the keyway. The use of modified shoulders may prevent this from happening.

In the minimal-movement method, material is removed from the tip and shoulder. This makes the method work but also inserts the key far enough that in some cases affects the keyway. This is due to the key material getting thicker as it reaches the bow. In the photo, this can be seen around the edge of the keyway.

Many unskilled attackers may attempt to bump unbumpable locks. This will probably damage the lock and borders on breaking the lock completely. In the photo, an EVVA 3KS wafer is shown after an bumping attempt. The wafer arm has broken off and a large dent is present, this lock was non-functional after this.

In this photo we see the cylinder from the failed bumping of an EVVA 3KS. The serious damage to the walls of the cylinder is due to the wafers slamming against the cylinder when bumping was attempted.

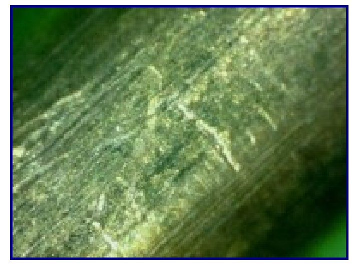
Manipulation-based impressioning works by taking a blank key that fits a target lock, applying extreme torque to the key (thus binding components), and manipulating the key blank in order to produce marks on the key. This is correct for pin-tumbler locks, but the actual process varies for different lock designs. The theory behind impressioning is that components at the wrong position will bind and become immobile. When the soft brass key contacts the immoble components, a mark should be produced. When a component is properly positioned it should no longer bind and thus no longer leave marks. The blank is used to gather marks, then filed in those positions. This is repeated until all components are in their proper position and the lock opens.

Because this type of manipulation is stressful on the key and cylinder we expect to find various types of forensic evidence. Namely, it is expected that the forceful binding of bottom pins, all of which are raised at or above shear line, to cause marks. We may also find material transfer from filing the key if the attacker is not careful to properly clean the key after each filing.

There are variations on the manipulation process that use pressure responsive materials, such as lead, tape, or plastic to facilitate the process of impressioning. In these cases we may also find material transfer as the soft materials rub against the keyway and inside of the plug.

Of course, the key used in manipulation-based impressioning will provide a good deal of forensic evidence.

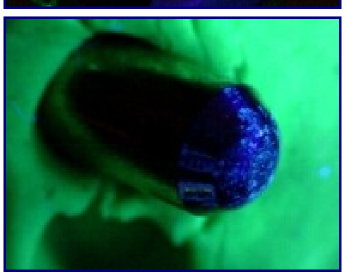
Forensic Evidence



Because we are forcibly binding bottom pins at or above the shear line we expect to see marks on the pins where this occurred. In the photo we can see several marks where the pin was bound against the plug in the form of straight lines sheared into the pin. (Note: the scratches to the left are pick marks)

Sometimes, impressioning marks are so clear that we can count the rounds of impressioning. If marks are far apart the forensic locksmith can also measure the distance between them. This may indicate a more skilled attacker if they are using factory depth increments to speed up the impressioning process.

The key blank may be specially prepared for impressioning via manipulation in a variety of ways. One of the possibilities is the use of Ultraviolet ink and an ultraviolet light source. This is an interesting technique, but as you can see in the photo it leaves ultraviolet ink residue on the face and insides of the lock.



When using UV impressioning, UV ink is reapplied each time the blank is filed. In turn, the pins will have a large amount of UV reside on them. Notice the obvious key pattern of UV ink across the sides of the pin. In addition, the UV pen fibers may have been stuck to the key and left behind on the pins or the plug walls.

Decoding Principles

Keys can be directly examined and decoded. Key decoding focuses on identifying the pattern of bitting cuts on the key. These can be determined by looking at the code numbers stamped on the key, or through direct measurement of each cut with a ruler, micrometer, or caliper. These measurements are used to determine the manufacturer's bitting code so that a key may be easily made. Sophisticated locksmithing tools are available that will automatically identify the bitting code based on the cuts and keyway profile of the key. This is the most basic of decoding methods, and may be problematic with high-security keys that have advanced features like sidebars, angled bitting cuts, moving parts, or magnetic/electronic components.

Components inside the lock can also be decoded through invasive, manipulative tools. These tools have radically different designs, and are generally specific to particular brand or model of lock. Most manipulative tools focus on measuring each component to determine: weight, range of movement, shape, spacing, and alignment. Many manipulative decoding tools resemble traditional lockpicking tools with the addition of a measurement device. Opening the lock via lockpicking is sometimes a pre-requisite to decoding the components. Many tools also decode the lock as they pick it. The standard tubular lockpick and the Sputnik tool are the most popular examples.

Disassembly of the lock can also be done to directly measure all internal components. This can be a complicated procedure depending on what type of lock it is and how it is installed. This process usually requires the lock be compromised first so that the door can be opened. Facilities with lax security measures may leave doors unlocked and unguarded, allowing someone to quickly remove, disassemble, and decode a lock. Reassembly and reinstallation of the lock is equally important, and if done incorrectly can cause the lock or proper key to no longer function.

Visual/optical decoding focuses on observation or surveillance of the key or internal components without needing to invasively manipulate them. A photograph of a standard key's bitting is enough to decode the bitting code. Surveillance may be used against combination locks to observe the correct combination being entered by an authorized user. Optical decoding uses tools like borescopes or otoscopes to look inside the lock at the internal components. Optics can be used to look at the size, shape, color, alignment, and spacing of internal components.

Radiological imaging is a form of surreptitious decoding that uses penetrating radiation (X, beta, and gamma rays) to "see" inside the lock or safe, revealing the proper positions of components. This is most often used against rotary combination locks to determine the position of each gate in the wheel pack. While very effective against many combination locks, it is expensive and only used by medium-high skill attackers.

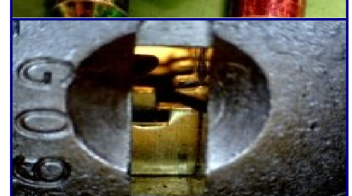
Thermal imaging is another form of surreptitious decoding that uses special devices to look at thermal residue left on keypad or pushbutton combination locks. This reveals buttons recently pushed, but may not directly reveal the combination sequence. Like radiological imaging, this is generally not used by low skill attackers.

As you can see, decoding is a vast array of techniques with forensic evidence equally varied. Manipulation-based decoding tools provide forensic evidence that is similar to lockpicking, but may vary depending on the specific techniques. Examination of keys may leave forensic evidence depending on the type of tools used. Visual, optical, radiological, and thermal decoding are all considered surreptitious and leave no lock related forensic evidence.

Forensic Evidence

Colored components are a red flag that optical decoding may be possible. The colors signify the size of components, and can be viewed with a borescope or otoscope to decode the lock. Colored pins are rare in factory-original locks, but are popular in many do-it-yourself lock repinning kits.

Low security wafer locks can be visually or optically decoded simply by looking at the size of the wafers. Unlike pin-tumbler locks, wafers block at the same position outside above the plug. Keying is made possible by varying the amount of material in the middle of the wafer, causing it to be raised high or lower by a key.



Keypad-based combination locks can often be visually decoded based on wear. In the photo, the worn down numbers help to reduce the search space to only a few combinations of numbers. It is possible that the combination is meaningful to the

owner, such as their birthday year or lucky number.

Anti-Forensics

Forensics is a never ending cat and mouse game. Investigators look for better methods to determine what happened while attackers are look for better ways to cover their tracks. This section discusses so called 'anti-forensics,' various techniques and methods to conceal evidence of entry.

Entry techniques that leave no forensic evidence are known as surreptitious entry. While technically surreptitious and leave no forensic evidence, the act of using them may leave non-lock evidence. When we talk about "no forensic evidence", we mean as it relates to the examination of the lock, safe, or related components, other forensic evidence may still be available. For example, forensic evidence may be found in the form of fingerprints on a safe dial, hair, fiber, footprints, surveillance, et cetera.

In many cases the forensic locksmith is asked to provide an assessment of how plausible certain surreptitious entry techniques are against a given lock. This can be done through a series of laboratory tests, an analysis of the required skills, tools, or money required, and examination of the installation and configuration details of the lock. Cases of completely surreptitious entry are viewed by the investigators on the basis of what facts and logical conclusions present themselves.

Anti-Forensic Materials

The idea of anti-forensics materials in tools is a popular but not well researched (publicly) area. Lockpicks made of soft materials such as wood or plastic would, in theory, not leave any marks on the considerably stronger brass, nickel-silver, or steel components. While they sound great in theory, they are considerably harder to use in practice. Tools made of these materials are considerably weaker, less maneuverable, and more prone to fracture or breakage than the steel normally used in tools. These types of tools also exhibit drastically reduced feedback capabilities, important in many covert entry techniques, when compared to metal. Coating standard tools with other materials has also been attempted, with limited success. The best example is teflon coated lock picks, which do not leave traditional marks, but still leave marks.

I have been doing my own research into anti-forensics materials and find that most of them are lacking in all areas. To date, no materials that I have tried have been successful at both picking a cylinder once and not leaving any forensic evidence. So far I have tried:

- Carbon Fiber
- Fiberglass
- Brass
- Teflon coated steel pick

These materials have also left various forensic evidence.

One area that anti-forensic materials may be used in is the production of non-metal keys. Plastic keys are considerably easier to use than plastic picks because their size is much bigger than the common lock pick. Research into this area is rather sparse, as well, with the use of a plastic pen casing to surreptitiously open low-security tubular locks being the most notable example.

Another area is "glue gun" shoulders for bump keys. Bumping can cause pronounced, noticeable damage to the face of the lock. This damage can be reduced or eliminated by removing the shoulder of the key and replacing it with a glue gun stick, an inexpensive piece of soft plastic. (Note: This technique does not remove the forensic evidence found inside the plug or on the pins.)

Tryout Keys

Tryout keys are a surreptitious entry technique against pin-tumbler and wafer locks. They use a series of keys with varied cut and spacing configurations to exploit poor tolerances in low-security, master keyed, or extremely worn locks. A tryout key works by being inserted into lock and jiggled back and forth in order to attempt to align components at the shear line. To assess the effectiveness of tryout keys against a particular lock, 25 random keys for the lock are produced. The forensic investigator attempts to use these keys, inserting and jiggling them, to open the cylinder. The investigator can provide a reasonable assumption on their effectiveness based on how many were able to open the cylinder.

Visual/Optical Decoding

Visual and optical decoding of the combination, key, or internal components is another form of surreptitious entry. In this case, observation, surveillance, photography, or optical devices are used in various ways. In all cases, a key can be produced with the information gathered from decoding:

- Observation of a key's bitting depths or direct code.
- Photograph of a key's bitting depths or direct code.
- Observation/surveillance of a combination lock sequence being entered.
- Visual decoding of a key impression.
- Visual decoding of a master key system through the analysis of system key(s).
- Optical viewing of component positions.
- Optical viewing of component shapes (Medeco Biaxial, for example).
- Optical viewing of component coloring (indicates depth).
- Thermal viewing of electronic keypads.
- Radiological imaging.

When we speak of optical viewing of components we're usually referring to invasive tools such as a borescope or otoscope.

There are several high-profile anecdotes which illustrate the power that visual decoding has. The Diebold company once published a picture of a key used for voting machines across the country on their website. This key (wafer) was visually decoded and it was found that it could be used to gain access to every single voting machine in the country. In the great story of the Antwerp Diamond Heist, thieves obtained the combination sequence by installing surviellance above the combination lock on the overhead alarm used above the safe door.

Combination Manipulation

Almost all low-security combination padlocks and Group 2 safe combination locks are subject to compromise by manipulation. Manipulation may be seen as a method of decoding where diagnostic information is taken through the use of the combination dial in order to determine the proper combination sequence. Manipulation is commonly (though erroneously) portrayed in many films, and is indeed an effective method against many combination locks. Group 1 or Group 1R safe locks are considered "manipulation resistant" because of various design changes the limit the effectiveness or drastically increase the time required to successfully perform manipulation.

Auto-dialers (or computer dialers, robot dialers) are machines that automate the process of manipulation either through sophisticated manipulation software or brute-force cracking of the combination. Auto-dialers may leave forensic evidence depending on how they are mounted to the combination lock and how long it takes to work. The process of auto-dialing accelerates wear on the lock components, and this may be detectable. The use of rotary combination locks with an electronic audit log may also be able to spot and prevent this sort of activity.

Radiological Imaging

Radiological imaging is a form of surreptitious decoding that uses penetrating radiation (X, beta, and gamma rays) to "see" inside the lock or safe, revealing the proper positions of components. This is most often used against Group 2 rotary combination safe locks to determine the position of each gate in the wheel pack. This is a surreptitious entry technique unless the use of such a device can be detected. In many cases, even if the ability to detect this form of entry is available it may be considerably expensive. The KGB is widely known to have used these devices when compromising American safes during the cold war.

The use of low-density wheel materials (such as Delrin) combats this attack. Group 1R safe locks are specifically designed to defeat various radiological attacks as well as provide manipulation protection.

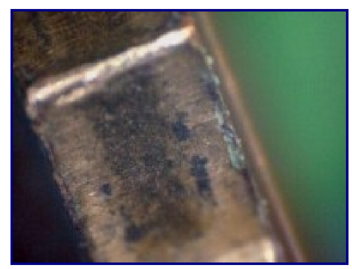
Surreptitious Bypass

There are some forms of bypass that may be surreptitious if used properly. Most padlock bolt shims are made of metal, but some low-security padlocks are of a poor enough quality that they can be shimmed with paper. This, of course, does not leave marks on the padlock bolt.

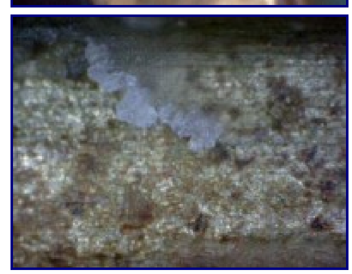
In the case of a thumbturn or lever (handle) lock, there are tools that will reach under the door and attempt to grab the thumbturn or handle and unlock or open the door. Depending on the design and material of the tool and the number of attempts it takes to open the door there may not be any forensic evidence. In this case, the forensic locksmith will note that the potential for this attack exists. If no other evidence is found it may be decided that this was one of the most probable methods of entry.

Material Transfer

Various materials are transferred to the key during use. Generally hair, fiber, and fingerprints will be examined by a crime lab. The forensic locksmith, however, may examine the findings of the crime lab to identify the uses of materials found on keys. Here we see a light green residue, which happens to be modeling clay.



In this photo we find small traces of white wax left in the warding of the key. Both this and the previous image indicate that the key has been impressioned (via copying). Through further analysis we may be able to link these and other materials to those found in a suspect's possessions.



Keys should also be viewed under various light sources to attempt and fight any material residue that may not be visible with the naked eye (or naked microscope?). In this photo, a key is being viewed under ultraviolet light to discover traces of ultraviolet ink along the key bitting area, indicative of impressioning via manipulation.

Bypass Principles

Attacks against the cam or actuator are a class of bypass that is surprisingly effective. In this attack, a poorly designed cam or actuator may be manipulated without affecting components. This vulnerability is somewhat uncommon, but extremely effective and easy to do when present. Because tools must generate a mild amount of torque as well as travel through the plug, they leave distinct tool marks.

Spring loaded bolts or latches are subject to an attack known as shimming. In shimming, a wedge is used to separate the bolt from the spring, or the bolt from the recess (such as in a door). The classic credit card trick to open doors is a popular example of this technique. Low-security padlocks are also commonly susceptible to shimming of the shackle. Shimming against doors is also known as loiding.

Locks that use a thumb-turn or lever handle on the inside of the door may be vulnerable to bypass. In this attack a tool is slipped under the door and attempts to swing and catch onto the thumb-turn or lever. The tool is used to turn or pull until the door is opened. This may or may not have forensic evidence, depending on the material of the tool, handle, and how many attempts are necessary to gain entry.

In automobiles, the door frame may be attacked with what is known as a air wedge. First, a wedge (usually plastic) is used to lightly separate the door from the frame of the automobile, then a deflated air wedge is placed in the opening. The air wedge is filled with air, causing it to expand, and the door is held open to allow a tool to be inserted to manipulate the inner unlocking mechanisms inside the vehicle. This technique is commonly used by locksmiths during automobile lock-outs.

The American 700 (old models) have a vulnerability that allows bypass via manipulation of the cam. Essentially, the cylinder is not required to move in order to actuate the cam. Tool marks left on the cam and back plate indicate that bypass was used as the method of entry. In response to the above attack American Lock (now owned by Master Lock) issued a hardware patch to prevent the bypass method. It is just a small metal disc, and in the photo we can see tool marks from where bypass was attempted. The 700 has since been redesigned because another attack against this component makes bypass again possible.

Excellent websites on lockpicking

http://www.iail.org	The International Association of Investigative Locksmiths
http://toool.us	The Open Organization of Lockpickers
http://www.ndemag.com	Free lockpicker / hacker magazine much like the Paranoid
http://www.theamazingking.com	Great website about cryptgraphy and lockpicking
http://www.deviating.net	Lockpicking website
http://blackbag.nl	Lockpicking website
http://www.lockpicking101.com	Lockpicking website
http://www.lockwiki.com	Interactive locksmithing site with excellent beginners introduction.

Thank you for reading our tenth edition

Visit Resist.com to buy future and archived editions.

Sure you can trust the government, just ask an Indian!
We work with a separate organization that allows us to maintain our privacy and acts as a cashier for sales and donations. Please refer to THE PARANOID NEWSLETTER in all your correspondence, otherwise the staff will confuse your correspondence with another newsletter. Send email to TM_Metzger@yahoo.com (Note the "_" character is not a space) or send us snail mail with your donation and request for additional newsletters to:

Tom Metzger
P.O. Box 401
Warsaw, In 46581