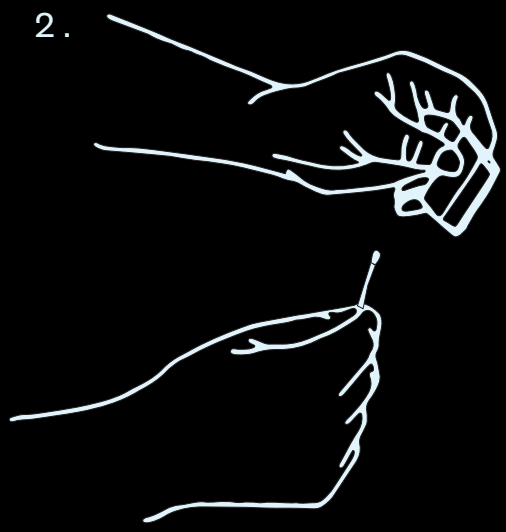
reason

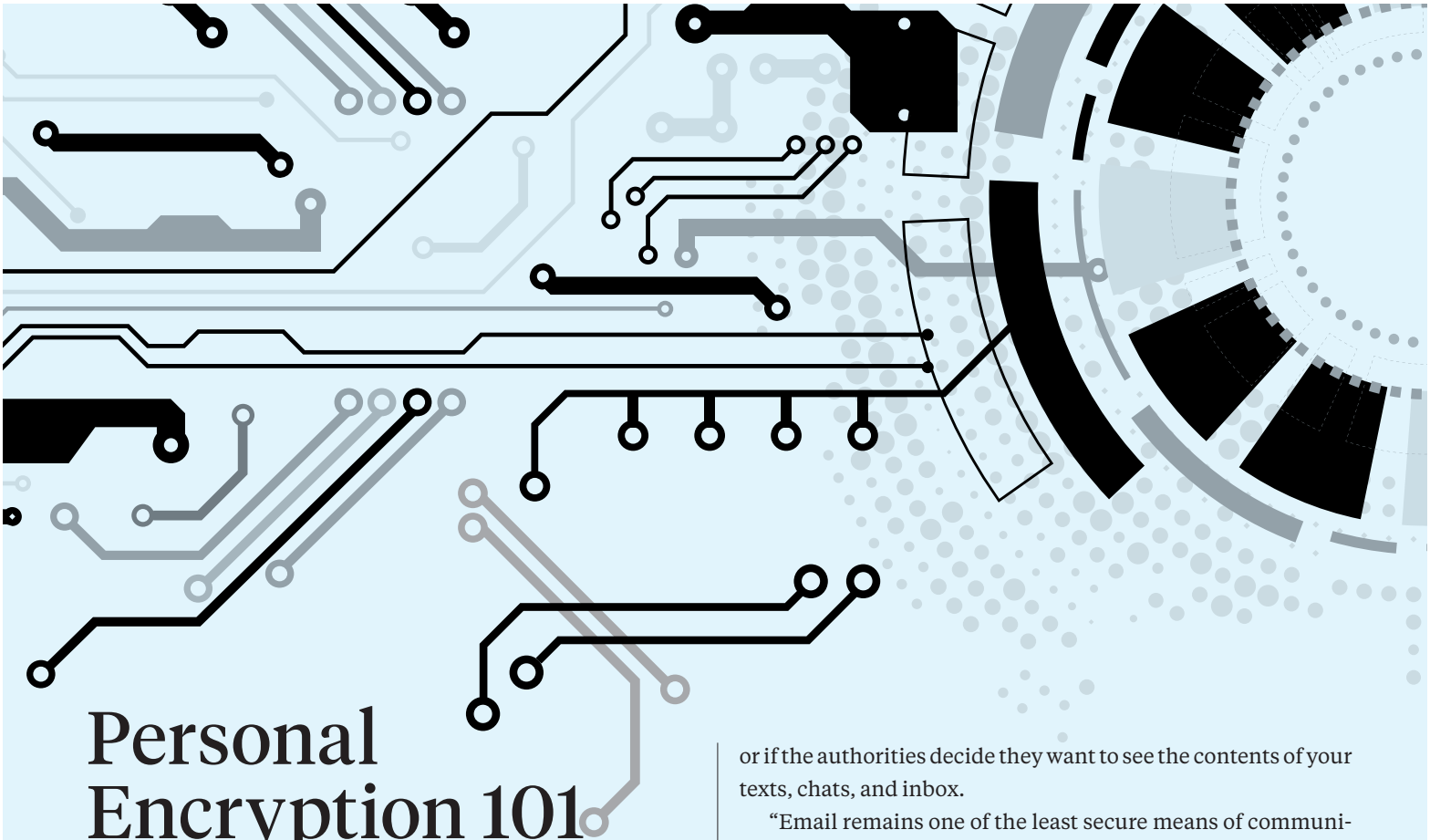
1.

2.



3.

4.



Personal Encryption 101

A BEGINNER'S GUIDE TO PROTECTING YOUR MESSAGES, MASKING ONLINE MOVEMENTS, AND STEERING CLEAR OF DIGITAL SNOOPS

ELIZABETH NOLAN BROWN

IN 2016, A lone Romanian hacker going by the name Guccifer 2.0 claimed credit for the leak of sensitive internal Democratic National Committee emails. But the would-be hacker celeb's story was quickly debunked by a single nonmasked login from a device at the headquarters of the Russian intelligence service, thus turning what looked like a tech security problem into an international spy scandal. That high-stakes slip-up shows just how stringent one must be to get away with online chicanery these days, when one's every login and keystroke can be tracked through an array of digital identifiers.

But you needn't be engaged in espionage, or anything illegal, to benefit from better digital privacy practices. From surveillance-happy state actors and data-harvesting advertisers to popular email clients, social media apps, and other ubiquitous web tools, there are plenty of potential peepers looking to glimpse your digital data (and potentially share it with or sell it to others).

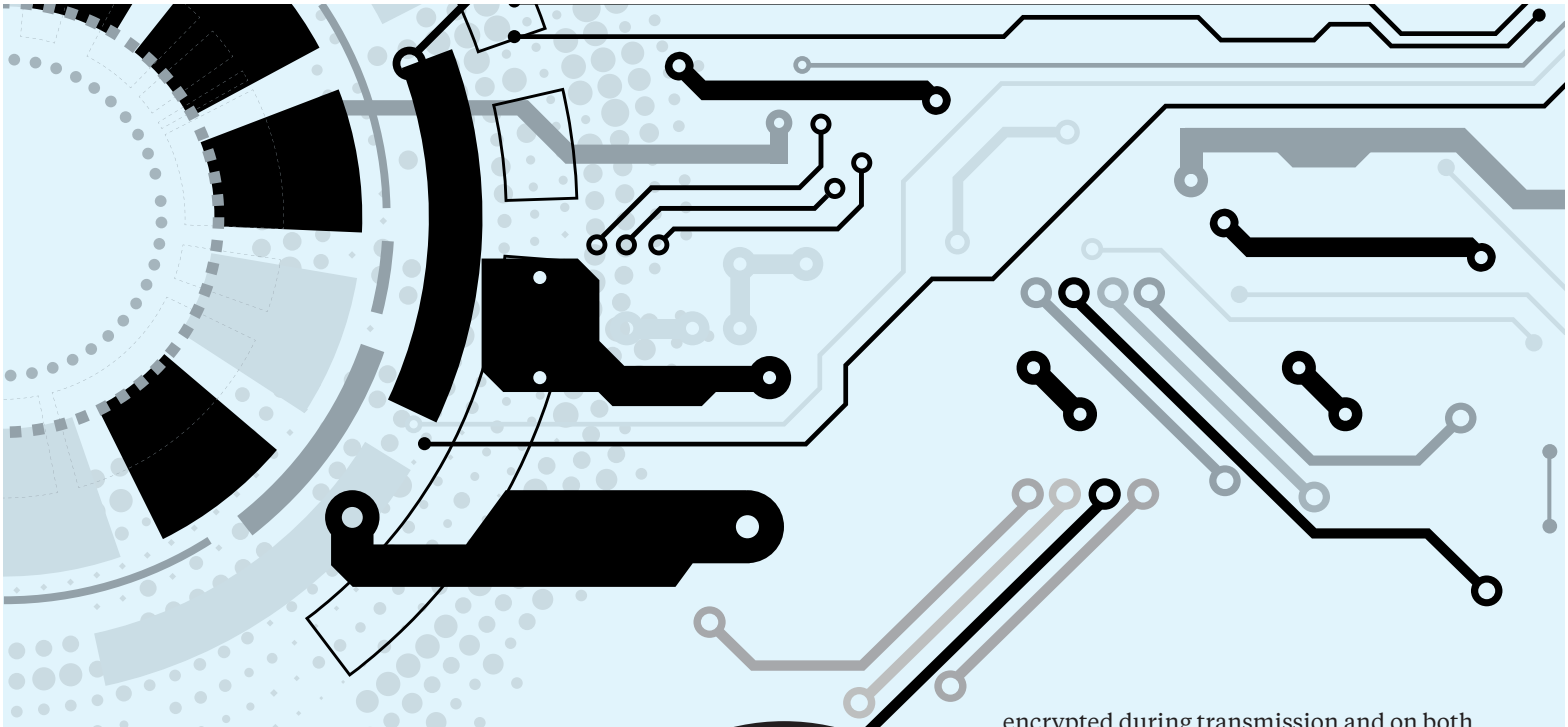
Traditional privacy protection methods—strong passwords and security questions, plus two-step authentication—are your first line of defense. But they may not cut it if convoluted terms of service give sites more leeway with your data than you realize, if hackers breach the servers where companies store your data, or if the authorities decide they want to see the contents of your texts, chats, and inbox.

"Email remains one of the least secure means of communication, and has been likened to sending a postcard—basically anyone along the way who's interested can read the contents of a message," writes journalist Jonas DeMuro in the U.K.'s *TechRadar*. This is because "an email is not a direct communication, but rather goes via several intermediaries...with multiple copies of the message stored at each server, and further copies on both the sender and recipient's computer." *Deleting* something, in other words, doesn't come anywhere close to actually eliminating it.

Email also typically lacks strong protections against access by law enforcement agencies. Under the Electronic Communications Privacy Act, authorities can obtain message content without a warrant after 180 days. (Many providers won't agree to give up your data without a warrant, but they could.)

True online anonymity requires elaborate measures—think a separate device for the anonymous identity, separate phone numbers, use of a virtual private network (VPN) for every login. But most people don't need, or even want, *total* anonymity.

For most of us, privacy can be drastically improved with a few simple (and free) tweaks and tools. In countries like Turkey, where many websites are censored, they can be essential for the most basic online communications. But even in the U.S. and other Western democracies, these services are enjoying a surge in popularity, thanks to sudden skepticism about the data-security practices of social media giants and increasingly invasive government speech codes for the digital sphere. If you too are ready to take back some of your online privacy, this is a guide to getting started.



TO KEEP YOUR EMAIL SAFE

ENCRYPTION, ENCRYPTION, ENCRYPTION. Encrypted email services scramble your data so only you and the message recipient(s) can view a readable version. The undecipherable copy is what passes through and gets stored on the email client's servers, so even if they're hacked, subpoenaed, or cursed with nosy employees, your messages can't be read.

***REASON*'S PICKS**

Best: ProtonMail

Still good: Tutanota, Mailfence, Disroot

Avoid: Gmail, Microsoft Outlook, Yahoo, Hotmail, AOL

The crowd favorite in this arena so far is **ProtonMail**, a Switzerland-based company that says it keeps its primary data center "at a secure facility 1 km under a mountain."

"Because data is encrypted at all steps, the risk of message interception is largely eliminated," the ProtonMail website notes. Emails are first scrambled on the user side, with a key the company can't access—which means even if it wanted to decrypt your mail, it would not have the technical ability to do so. (It also means that if you forget your password, you lose all your previous data.)

ProtonMail promises not to track user information, including metadata or IP addresses, a numeric designation that identifies a location on the internet; doesn't require personally identifiable information to create an account; and features an optional "self destruct" setting when emailing other ProtonMail addresses that automatically deletes a message from both the sender's and the recipient's accounts after a chosen interval. Basic accounts are free and come with 500 MB of storage. Paid accounts ($48 to $288 per year) offer between 5 GB and 20 GB.

In general, ProtonMail looks and works like regular email. Messages sent between ProtonMail accounts are automatically encrypted during transmission and on both ends. When communicating with a non-ProtonMail user, you must provide a security key if you want the email to be encrypted throughout transmission. Mail recipients will be directed to the ProtonMail site to decrypt the email and reply securely.

Over the past few years, ProtonMail has been rolling out an array of new security features, including encrypted contacts for Android and iOS devices and a service called ProtonMail Bridge, which syncs (paid) ProtonMail accounts with traditional desktop email clients such as Microsoft Outlook.

In addition to all this, the company espouses an old-school anarchic internet attitude that's a welcome contrast to most mainstream email providers. As federal authorities damn encryption as a threat to national security, ProtonMail has pushed back against the idea that only the lawless should embrace anonymous communication tools. "It is incorrect to say that using ProtonMail implies you have 'something to hide,'" said founder Andy Yen in a recent blog post. "ProtonMail provides more security and privacy compared to Gmail or other email services, and security is desirable for practically anyone that uses the internet."

Yen noted that "emails, encrypted or not, can be subject to subpoenas." But at least with services like ProtonMail, "it is not possible to obtain them from the service provider, and instead the subpoena must be served to the individual or organization under investigation."

Another service that gets good marks from privacy types is **Tutanota**, a German company that offers end-to-end encrypted email with 1 GB of storage for free, plus a paid version for those who need more space, multiple addresses, and other features.

Joanna Andreasson. KrulUA/iStock

As with ProtonMail, email between Tutanota accounts is always encrypted. Sending encrypted messages to a non-Tutanota account requires setting a password and providing it to the recipient in a separate, nonencrypted email. The recipient will be prompted to visit the Tutanota site and enter the password, and then he or she can read the message.

Like ProtonMail, Tutanota's rhetoric is admirably lofty. Last summer, co-founder Matthias Pfau told *TechCrunch* that "we at Tutanota see ourselves as Freedom Fighters. We believe in human rights such as our right to privacy and freedom of speech. But as these rights are being cut by governments around world, we need to fight back."

Belgium-based **Mailfence** operates much like ProtonMail and Tutanota. Its more robust accounts can be paid for using bitcoin. **Disroot** offers encrypted email as well as cloud storage and a host of other services, including a message board, a Twitter-like social media platform called Diaspora, and a browser-based text editor that can be set to "burn after reading," leaving no trace of the decrypted document on either the author or the reader end. The all-volunteer, Amsterdam-based team says it aims to create digital tools that are "open, decentralized, federated, and respectful towards freedom and privacy."

TO CHAT, SEND PHOTOS, OR MAKE CALLS SECURELY

ENCRYPTION IS ALSO the answer for protecting the secrecy of your more casual communications. There are several popular services right now that allow for the easy exchange of encrypted chat—consider this your alternative to both texting and the likes of Gchat, Facebook Messenger, and similar direct-messaging services—as well as offering ways to make calls and privately exchange photos or videos. The only catch is that your contacts are limited to those who are also using a particular service or app.

Which one you choose—**Signal**, **WhatsApp**, and **Telegram** are the three most popular—should depend on where you live, which apps are in use among your social and professional networks, how much security you're willing to exchange for other positive attributes, and how much faith you put in proprietary data systems. Your individual privacy concerns come into play as well: Is it government or service-provider snooping that concerns you? Are you trying to prevent people in your household from reading your texts? Do you need to be able to verify the identity of those you're messaging with? Do you mind giving out your phone number?

Telegram is not built on open-source software—a major strike against it, according to some privacy hawks—and the use of a proprietary encryption process is another potential black mark. The London-based service has also run into trouble in such countries as Iran and Russia, where authorities have demanded Telegram turn over info that would let them decrypt all user emails—Telegram declined—or moved to block the service altogether. But it has around 200 million active users per month and boasts large user bases in former Soviet Union countries and the Middle East, which can make it attractive for people with a lot of contacts there. And founder Pavel Durov at least pays lip service to the privacy-minded ethos that ProtonMail and Tutanota tout. "We don't regard Telegram as an organization or an app," he wrote in a March blog post. "For us, Telegram is an idea; it is the idea that everyone on this planet has a right to be free."

Privacy clearinghouse PrivacyTools.io recommends against both Telegram and WhatsApp, a similar (and even more popular) chat platform. In general, the biggest complaint about the latter is that it collects user metadata—and that its parent company is Facebook.

The Electronic Frontier Foundation (EFF) has said on its blog that if pressed, it would recommend either WhatsApp or Signal, though it notes that it's difficult to "make a recommendation without considering the details of a particular person's or group's situation."

Overall, Signal gets the best ratings from the widest array of groups and people, especially if you're looking for strong security. Both Signal and WhatsApp "employ the well-regarded Signal protocol for end-to-end encryption," EFF noted, but "Signal stands out for collecting minimal metadata on users, meaning it has little to nothing to hand over if law enforcement requests user information. WhatsApp's strength is that it is easy to use, making secure messaging more accessible for people of varying skill levels and interests."

TO BROWSE THE INTERNET ANONYMOUSLY

MOST BROWSERS NOW offer an "incognito" or "private browsing" mode that doesn't log your search or site-visiting history. But these functions only mask your trail locally (i.e., the pages you visit in an incognito window won't show up when you check your browser history). They don't mask your IP address or hide your identity from sites you visit.

No one app or fix will let you browse online totally anonymously, but the most simple and comprehensive option

is to download the **Tor** browser. Tor—which works on Windows, Mac, Linux, iOS, and Android—is an open-source, modified version of the Mozilla Firefox browser that comes pre-installed with all sorts of privacy features. The bottom line is that it can keep your computer's address from being logged by websites.

"The Tor network is a group of volunteer-operated servers [that] employ this network by connecting through a series of virtual tunnels rather than making a direct connection," the Tor website explains. This lets people "share information over public networks without compromising their privacy" and serves as "an effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content."

To supplement Tor, savvy web surfers may want to use a virtual private network (VPN). Normal browsers let your internet service provider (ISP) see every site you visit, in addition to your computer's personal IP address being visible to the sites themselves. VPNs prevent this by filtering your traffic through their network and serving it up with a new, masked IP address.

This means that your ISP records you going to the VPN but not to the sites you visit thereafter. In addition, the sites you visit see the IP assigned to you by the VPN, not your actual information. This can be especially useful for getting around geography-based content filters, like China's ban on many American sites and apps (often referred to as the "Great Firewall") and Russia's ban on everything from Telegram to, temporarily, Google.

The VPN also encrypts your traffic, so it's not accessible the way your browser history on a normal browser would be. Using a VPN is similar to using web proxy servers, which serve as a screen between your computer and your internet activity, except that VPNs also mask your identity when interacting online with games, torrent apps, and the like.

A word of caution: A VPN alone will not keep your emails safe if you're using a traditional email client. It will mask you from your ISP, but unencrypted copies of your messages will still be stored on email client servers.

VPN clients can be downloaded for use on computers, tablets, and smartphones. Some free VPNs that get consistently good reviews are CyberGhost, TunnelBear, and Windscribe. PrivacyTools.io also has put out a list of recommended VPNs, all of which are based outside the U.S., use encryption, and accept bitcoin. **ProtonVPN** (associated with ProtonMail) is the only one of the most highly rated services that's also free; the others range from around $35 to $125 per year.

Regular browsers *can* be configured to offer more privacy through the use of various plugins. PrivacyTools.io offers recommendations on that score as well. Of the most well-known browser options, **Mozilla Firefox** and **Brave**, from former Mozilla CEO Brendan Eich, are arguably strongest when it comes to security.

***REASON*'S PICKS**

Best: Tor + ProtonVPN

Still good: Brave, Mozilla Firefox (with fixes), other VPNs

Avoid: Google Chrome, Safari, Internet Explorer

TO KEEP YOUR SEARCH HISTORY SECRET

WHEN USING TYPICAL search engines like Google, Yahoo, and Bing!, clearing your search history from your browser window doesn't mean it's actually gone forever. Your search log is stored by the search-engine company in question. To search without leaving a trail, try **DuckDuckGo**, which doesn't track any user data, or **StartPage.com**, which lets you use Google's search engine without being tracked by the tech giant.

TO MAKE YOUR GO-TO TOOLS MORE SECURE

GMAIL OFFERS EMAIL encryption under some circumstances—if a user is on a Chrome browser or using a Gmail app and is emailing another Gmail address. But as *TechRadar* notes, "Google has become the Big Brother of the internet, and is known for reading user's messages, all in the name of targeting them with more relevant ads; there's privacy, and there's Google's idea of privacy."

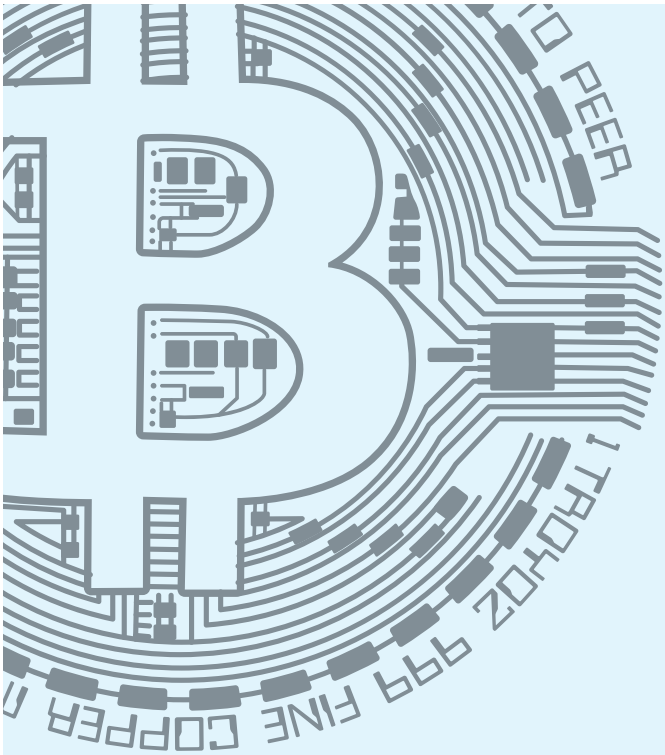
Microsoft Outlook also has an encryption option, but it only works in limited instances.

If you're using a desktop email client, you may be able to use **ProtonMail Bridge** to add a layer of protection. The service integrates with Outlook, Apple Mail, Thunderbird, and similar options, serving as "a bridge between the unencrypted and encrypted worlds in the sense that it allows your average user to benefit from the added security and privacy of end-to-end encryption without having to make any changes to their email usage behavior," ProtonMail's Yen explained in a statement.

TO MANAGE ALL YOUR PASSWORDS

THE BEST ENCRYPTION plans in the world don't mean anything if you forget your passwords or if your passwords aren't secure. Consider ditching options such as iCloud Keychain, 1Password, and LastPass in favor of **KeePass**, a free, open-source password manager with strong encryption game.

ELIZABETH NOLAN BROWN is an associate editor at *Reason*.



3 Steps to Buy and Store Bitcoins Anonymously

JIM EPSTEIN

BITCOIN IS THE first uncensorable digital currency: When it moves between buyers and sellers, there's nothing anyone can do to stop it. The now-shuttered online marketplace Silk Road couldn't have existed before bitcoin, because it's unfathomable that Visa, Mastercard, or PayPal would approve transactions on an e-commerce site for buying and selling illicit drugs.

Bitcoin is often mistakenly described as a "fully anonymous" cryptocurrency. In fact, while global superpowers can't prevent you from spending your bitcoins, that doesn't mean they can't figure out what you bought. More than 100 Silk Road users have gotten into trouble with law enforcement since 2012, and the Snowden leaks revealed that the National Security Agency has worked to uncover the identities of other bitcoin users as well.

Though you don't need to give up your real name to use bitcoin, transaction histories are fully visible in an online ledger called the "blockchain." Skilled digital forensics investigators can link your real identity to a bitcoin address by extracting information from pervasive "web trackers." These are hidden programs installed on your computer that capture information about your browsing and purchasing habits. Trackers, which are used by Facebook, Google, the FBI, and all sorts of malicious actors, can also record an IP address, the numeric code that identifies a home internet network. "Anonymity is misrepresented in popular culture…it's not an absolute," cryptocurrency researcher and security consultant Kristov Atlas writes in his self-published 2014 book *Anonymous Bitcoin*, a practical guide to concealing your identity. "The question at any given time is not, 'Am I anonymous?' but rather, 'How anonymous am I, and to whom?'"

There's no such thing as perfect anonymity, but a handful of best practices can go a long way toward shielding your transactions from government spies and other malevolents.

STEP 1: HOLD YOUR OWN BITCOINS

DON'T KEEP YOUR bitcoins on a custodial exchange such as Coinbase. These sites store your identity and may share it with law enforcement agencies, making transactions about as private as mailing a personal check with a return address. Instead, set up a bitcoin "wallet"—a software application that enables you to send or receive bitcoins in a peer-to-peer fashion, directly from your own computer. With a wallet, the secret codes required to spend bitcoins aren't stored by a third-party company or somewhere in the cloud. You maintain them yourself.

Atlas recommends running your bitcoin wallet on a cheap, dedicated PC laptop with the open-source Tails Linux operating system, which makes internet use hard to track. Tails Linux is designed to run off an external USB drive. (Since your laptop won't be functional until you have a working operating system, start by downloading Tails Linux on a different computer and saving it to your external drive.) Every time you finish using your dedicated bitcoin laptop, turn it off, unplug it, and disconnect the battery. This creates a fresh, anonymous session for next time that throws off trackers.

Electrum is an excellent bitcoin wallet that comes preinstalled on Tails Linux. Supplement it with a hardware USB device like a TREZOR or a Ledger Nano S, which add additional security layers that make it harder for an attacker to steal your bitcoins. The extra device will also help you detect if malware that compromises your anonymity somehow made it on to your computer. You can set the Electrum wallet to open only if one of these devices has been inserted into your computer and verified with a pin.

STEP 2: BUY BITCOINS IN PERSON

START THE BUYING process with the anonymous Tor internet browser, which comes preinstalled on Tails Linux. (You can download Tor on any computer, but you're less likely to be tracked if you use it on your dedicated bitcoin laptop.) Navigate to LocalBitcoins.com to look for a nearby bitcoin seller.

Joanna Andreasson

Don't use your real email account to register. You can generate a temporary, anonymous email address using a service like Dispostable.com.

Meet your seller at a coffee shop with a public WiFi network. Bring your laptop, and pay with cash. Once you're there, with a click of the mouse in your bitcoin wallet, you can generate a "receiving address"—an alphanumeric code that's the equivalent of a bank routing and account number—which the seller can enter or scan into his or her wallet to execute the transfer. Arrive in a borrowed vehicle or park far away. Don't give the seller your cellphone number, and don't show him or her pictures of your kids while waiting for your multiple transaction confirmations.

STEP 3: BURY YOUR TRAIL WITH A BITCOIN MIXER

TO OBFUSCATE THE movement of your funds, use a bitcoin "mixing" service. These are websites that accept your bitcoins and send you back different bitcoins that have no connection to your previous activities. It's like swapping cash for bills with different serial numbers. To make the transaction record harder to follow, mixing services will generally send the "clean" coins back to you in multiple transfers over a staggered time period.

The first step is to use your bitcoin wallet to generate several receiving addresses. (Again, a "receiving address" is the equivalent of a bank account and routing number—but bitcoin allows you to generate a fresh code with every transaction for better security.) Enter your receiving addresses into the mixer's website so it knows where to send your money when the time comes. Next, enter the receiving address of the mixer service into your bitcoin wallet. Execute the transfer.

After the payment is confirmed, the mixing service will send back the clean currency. Some services let you specify the intervals in which the payments will be made.

Bitcoin mixers do have downsides: Their fees can run as high as 3 percent, and they involve a degree of risk. You're trusting that the service won't maintain a record of your activities and that it won't abscond with your funds. But if you care about anonymity, mixers are an important tool for covering your tracks.

Take precautions, like using an established service, and test it with a small amount of currency before risking a large sum. The review site Darknetmarkets.co currently recommends Coinmixer.se, Helix, and Bitcoin Blender. Keep in mind, however, that bitcoin mixers can shut down or be compromised—a service that's reliable today won't necessarily stay that way. With bitcoin, you're in control of your own money. Use that power with care and caution. ⓡ

JIM EPSTEIN is managing editor of Reason TV.

To Spy on a Cheating Spouse

USE SOFTWARE, NOT GADGETS.

DECLAN MCCULLAGH

IN THE UNFORTUNATE event that your marriage does not last, it may at least end amicably. Or it may not, in which case its final days might need to be accompanied by the kind of aggressive electronic surveillance that once was used only by three-letter federal agencies.

But be warned if you're thinking about snooping on your spouse: A little-known section of federal law enacted in 1968, 18 USC 2512, makes it a crime to manufacture, assemble, or even possess any "device" that is "primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications."

Section 2512 goes beyond merely regulating whether any such device is used for good or ill. Instead, it's a far-ranging prohibition on everything, up to and including *advertising*, an eavesdropping device, based on the premise that unlawful wiretapping will be less prevalent if the tools are less available. Service providers like AT&T and Comcast are exempt. So, of course, are police, other government agencies, and their contractors.

The legislative history from the 1960s reveals that Congress wanted to ban products such as microphones disguised as wristwatches, as well as so-called infinity transmitters that send audio from a room over a phone line, giving the snooper an effectively infinite listening range. The danger of a "martini olive transmitter" was also cited, perhaps by legislative staffers who took the early James Bond movies a little too seriously. In the 1990s, federal prosecutors successfully invoked this law against The Spy Factory, which operated 16 retail stores that sold bugging and wiretapping equipment to the general public.

But thanks to Section 2512's practically antediluvian origins dating to the era of mainframes and punched cards, a loophole has been growing wider every year. That's because the pre-ARPANET statute only bans eavesdropping *hardware*. Congress revisited the law in 1986 as part of the Electronic Communications Privacy Act but ended up leaving Section 2512 intact.

If someone sells a laptop, phone, or home assistant with preinstalled software that spies on the user without his or her knowledge, that likely violates Section 2512 since those are

Joanna Andreasson

surely all "devices." Computer code is more slippery. One federal district court in Ohio concluded in 2008 that "software alone…does not fit into this definition."

In our increasingly networked world, this oversight offers a remarkable escape clause—and a useful reminder of the unreliability of politicians' predictions of the future. Today, any electronic device with a microphone or camera that's connected to a network can, with the right programs installed, become a bug far more potent than the infinity transmitter of the '60s. Yet restricting the use of computer programs raises First Amendment concerns: What about open-source projects? Could the state ban a book containing a printout of source code? (Undaunted, the U.S. Department of Justice invoked Section 2512 last year in its indictment of a researcher accused of creating and distributing the malware known as the Kronos banking Trojan. The case is ongoing.)

The upshot for those who suspect something is amiss in their relationships: If you're going to spy, do it via software.

Important and annoying lawyerly reminder: Installing snooping software may violate laws other than Section 2512, the relevant laws may change by the time you read this, and your local prosecutor may be good friends with your spouse, if not already sleeping with him or her. The bullet points below are guidelines, but you should proceed with care.

Recording conversations: Be selective about where you live. Some states, including California and Florida, require everyone in the conversation to consent. The rest allow surreptitious recording if one person consents, and fortunately, that one person can be you. Some apps, like Automatic Call Recorder for Android, can be configured to preserve every phone call you make and receive.

Tracking vehicles: GPS trackers are tiny magnetic transmitters, typically battery powered, that you can buy for as little as $30 plus a monthly fee. From an app or web browser, the user then monitors the vehicle's movements. To optimize for legality, be the sole owner of the target vehicle. Joint ownership is second best. If the only name on the title is your spouse's, don't say we didn't warn you.

Bugging backpacks: This little-known technicality lets you place a bug in your child's backpack to eavesdrop on nearby conversations. It can be legal, as long as you're in a state with one-party consent. The loophole exists because you, a parent, have the authority to grant consent on your minor child's behalf. New York's highest court ruled in 2016 that if a parent has "a good faith, objectively reasonable basis to believe that it is necessary," he or she may create a secret "audio or video recording of a conversation to which the child is a party."

Tracking phones: Surreptitious installation of spyware that tracks the whereabouts of your spouse's mobile device may not be prohibited by Section 2512, but it can violate other laws. Consent vitiates this problem, so create an account, with your spouse's knowledge, for the whole family to use—an iCloud account on iOS devices or a Google account on Android. For Apple products, make the iCloud-linked account the primary account, which allows you to use the "Find My iPhone" feature. On Android, go to "Accounts" under "Settings" and add the family account. At that point, as long as you're logged into the family account, you can type "find my phone" into Google and get a location fix. (Remember to turn on Location History, too.)

Watching online: Wiretap laws generally shield information while it's being transmitted. You're not the FBI, so don't engage in illegal wiretapping. But reviewing files stored on a shared computer used by both spouses isn't wiretapping. Nor would it be wiretapping if you happened to boost the size of the browser's cache, or made sure the browser history was automatically backed up on a regular basis.

Recording video: A surprisingly large number of spouses respond to suspicions that their partner is cheating by aiming a hidden camera at the marital bed. Proving adultery in the form of a H.264/MPEG-4 movie is not a good idea, however. If discovered, the best outcome is a sizable payment disgorged to the

LueratSatichob/iStock

Martini olive transmitters may be illegal (and imaginary), but Find My iPhone isn't.

spouse recorded in the act during civil litigation; criminal prosecutions are also likely. (One exception is Mississippi, where an ex-husband learned of his ex-wife's torrid lesbian affair with her new roommate. In an attempt to win sole custody of their minor daughter, he snuck up to the women's cabin and snapped photos through the window of an intimate moment. Although the man was promptly sued for invasion of privacy, the Mississippi Supreme Court ruled in 1999 that "reasonable people would feel [the ex-husband's] actions were justified in order to protect the welfare of his minor child.") Non-Mississippians might try the Reconyx MS7 camera instead. It's camo-painted, battery-powered, WiFi-enabled, and has the resolution and shutter speed to capture license plates. Stick it in a tree and aim it at your driveway, not your bedroom.

Protecting yourself: Do the opposite of the advice above. Your car's title should be in your name. Wipe your cellphone. Avoid shared computers. Use a Chromebook and turn on two-factor authentication. Consider additional security measures as they become available.

Perhaps the best advice is to think twice before going down this path at all. To the extent it lets you avoid the legal gray areas surrounding electronic surveillance, staying together can mean staying out of jail. ❶

DECLAN MCCULLAGH is a Silicon Valley writer, entrepreneur, and co-founder of Recent Media Inc. His wife is a lawyer at Google currently working on Google Search and Google Maps.

How to Get on a Jury

WHAT YOU DO ONCE YOU'RE THERE IS UP TO YOU.

MARK W. BENNETT

IF YOU WANT to serve on a criminal jury, the most important rule is this: Say as little as possible, with your words, your body language, and your appearance.

But why would you want to sit on a jury in the first place? Because in a criminal trial, if you can read and reason and resist being swayed by emotion, you will make a better juror than most of your fellow members of the community. A jury is the entity that acts as the voice of the community, and serving as a juror allows you to contribute to that voice.

You may also believe that the law under which the defendant is being prosecuted is an illegitimate use of state power. In that case, acting as a juror gives you the opportunity to exercise the power of *jury nullification*—finding the defendant "not guilty" regardless of whether the state has proven the accusation beyond a reasonable doubt.

This power to nullify an unjust law is as old as the institution of the jury; it's a practice rooted in the principle that a juror can and should reach whatever verdict her conscience leads her to, and that there is nothing the government, or anyone else, can do to stop her beforehand or punish her afterward. Of course, the state prefers to maintain tight control over trials. In most jurisdictions, defense lawyers are prohibited from telling juries about nullification, and judges and prosecutors will, if pressed, lie and tell jurors they may *not* vote to nullify. But that is all the state can do to try to stop it. Knowing the truth will keep you from being deceived.

In 23 years of criminal defense practice, I've tried more than 40 cases before juries that I've picked, plus assisted and watched many more lawyers' jury selections. I've made a study of the psychology and social dynamics of the process and taught the science and practice of it to countless lawyers across the country. I've learned that getting onto a jury to nullify illegitimate laws is easier when you understand the game that judges and attorneys are playing.

YOU ARE AN intelligent, opinionated person who wants to share with your fellow citizens the fact that they have the power to follow their consciences in arriving at a verdict. This is admirable. But if you succumb to the temptation to do so during jury selection, your chances of being chosen drop to nil.

We call the process of turning a group of community members into a jury of six or 12 "jury selection," but it is, by necessity, actually jury *deselection*. Each party can eliminate from the jury pool any person who has a bias for or against the defendant or a bias against any of the laws that are applicable to the case (this is a "challenge for cause"). Then each side can eliminate from the jury pool a fixed number of people for any reason at all, as long as that reason is not some form of proscribed discrimination (this is a "peremptory challenge"). The jury is the first dozen people (or half-dozen, in a misdemeanor case) remaining after both sides have exercised their challenges.

Lawyers find bias, and other reasons to strike jurors, in the things candidates say, the way they act, and how they look. As a practical matter, the first six or 12 people left after the lawyers have used all of their strikes are those who have kept their mouths shut and who appear ordinary.

Bias against "the law applicable to the case" is grounds for a challenge for cause, and while you and I know that jury nullification falls within the bounds of the law, the

system in practice does not recognize that principle. Judges will bar defense lawyers from even mentioning jury nullification, and judges and prosecutors will lie to jurors about that power (or right, if you prefer, since the people's *rights* are, of course, *powers* in relation to the state). A juror who expresses any understanding of her power to nullify bad laws will certainly be challenged by the prosecutor for cause and excused by the judge. Precedent is very clear that a willingness to nullify the law is a bias against that law, which is grounds for a juror to be stricken for cause.

The first challenge for someone who wants to be able to exercise his own sense of right and wrong in the jury room is—to be blunt—not to let the state know that he plans to do so.

Potential jurors are questioned under oath. As a philosophical matter, a person may feel that where the court and the state are lying to jurors about their power to nullify, jurors are justified in lying back. Perhaps you feel the power to nullify a law contains the power to nullify the oath to tell the truth, if that is the only way to exercise your right. But for our current purposes, let's assume that you are unwilling to commit perjury for the sake of nullification—that you believe lying under oath is a greater evil than being excluded from a jury because you know about your right to nullify bad laws. In that case, if the prosecutor or the judge asks you explicitly about your power to nullify—"Ms. Jones, do you believe that a juror has a right to follow her conscience rather than the law?"—you will answer truthfully, and your truthful answer will likely get you excused from the jury without further questioning.

Lawyers in jury selection have a lot on their minds, however. They are also often afraid of "poisoning the well" by eliciting ideas they don't want the other potential jurors to hear (including ideas about nullification). Now, this fear is irrational, since a juror who holds such a view but keeps it to himself will quietly carry the "poison" into the jury room. But even lawyers behave irrationally, and the chance you will be confronted with such a clear and direct question is slim.

Slightly more likely is a query such as, "By show of hands, who here believes in jury nullification?"

If you parse the question and the answer is inescapably "yes," then not raising your hand is concealing facts from the court while under oath to tell the truth. If you do raise your hand, there will be additional questions, which may lead the judge to conclude that you have a bias against the law and should be stricken from the jury. At the very least, your speaking up will give the prosecution a reason to exercise a peremptory challenge against you.

Better, from your perspective, that prosecutors should use a peremptory challenge than a challenge for cause, since they have an unlimited number of the latter but very few of the former. Still, the objective of this exercise is to get *on* the jury. Fortunately, unless the defense lawyer has telegraphed to the prosecutor an intention to rely on nullification (a bad idea if she actually plans to do so, though an excellent diversion if she does not), you probably won't get this question, either.

What is likely—especially with a case involving a relatively unpopular law, such as a law criminalizing possession of marijuana—is that the prosecutor or judge will ask a question along the lines of, "How many of you think that possession of marijuana should not be against the law?"

Your job as a potential juror is not to make the lawyers' jobs easy for them. If lawyers ask bad questions, you are not obligated to guess at what they actually meant, nor are you obligated to respond to the phrasing they should have used. ("The law in this state *is* that it is a crime for an adult to possess marijuana, anywhere, at any time. How many of you think that *should be* the law?") In this instance, you may think it fair to say that "not against the law" means never, under any circumstances, against the law. If you can imagine a situation in which it might be legitimately outlawed (in a school zone by a kindergartner?), you can honestly refrain from volunteering your view.

Assuming you are forced during jury selection to reveal your familiarity with the practice of nullification, you will not be serving on the jury. If, after learning that you know about it, the prosecutor is unwise enough to allow you to say more, you might as well take the opportunity to educate your fellow jurors about the doctrine. At least then you'll have accomplished something.

A juror who admits he is not able to follow the law is challengeable for cause. That's a freebie for the state. But *of course* you are able to follow the law; you just don't agree with the judge's and the prosecutor's assessment of the state of it. You don't have to share that last bit unless hard pressed; "I can follow the law" is often sufficient to keep a prosecutor from successfully challenging you for cause. If you can promise to "set aside your beliefs about jury selection and follow the law," so much the better. And what does "set aside your beliefs" mean? Who knows. They are formalistic magic words.

If your beliefs about drug laws are closely examined, you may honestly need to disclose that you would define "proof beyond a reasonable doubt" more strictly in a drug case than in some other cases. That likely won't lead to a challenge for cause: *Reasonable doubt* is a matter of personal judgment, each juror gets to decide what it means to him or her, and the prosecution isn't allowed to pick only people who agree with its definition of the term.

That pretty well covers the words you say: as few as possible, preferably none, while adopting the interpretation of each question that allows you the most freedom to keep your mouth shut. But you also need to consider the things you say without words. Most of us give away a great deal of information with our body language. Canny lawyers in jury selection are watching

your reactions—or have assistants doing so—and take that into account when making their peremptory challenges.

They also look at your clothing and accoutrements. So if you want to be on a jury, give them nothing to notice. Have a poker face, dress conservatively, and don't carry incendiary reading material, such as the latest issue of *Reason* magazine.

ONCE YOU GET on the jury, you will want to make the most of it. It may be that the defendant is accused of a crime that is *malum in se* (i.e., inherently wrong); that the police acquired the evidence without violating the defendant's constitutional rights; and that the evidence proves the government's case beyond a reasonable doubt. If so, you will follow the law and vote to convict. But if those conditions are not all true, and if conscience demands that you not convict the defendant, you can try to nullify. You may be able to get the rest of the jury to go along with you and hand down an acquittal.

By the time the presentation of evidence begins, all of the jurors have an opinion on culpability. As soon as they go in the jury room, they take a first vote to see where everyone is. Lawyers like to pretend that jurors then calmly and rationally deliberate, but the truth is that the majority pressures, cajoles, and browbeats the minority to switch sides. The evidence matters only insofar as any juror can use it to shore up her own position or give another juror an excuse to change his.

Each person's vote is a personal moral judgment, and nobody is entitled to pressure another person to go against his belief. But most people are not able to withstand the sort of social pressure that is put on them in the jury room, and so the side with fewer jurors in that first vote is likely to lose this battle. The greater the gap, the more likely are people in the minority to defect.

Criminal verdicts have to be unanimous, so if the jury announces that it cannot come to a decision, the court will take a few steps. First it sends them back for more deliberating. Next it gives them an "*Allen* charge" or "dynamite charge"—a set of instructions from the bench specifically intended to push the jurors to break the deadlock. Only when the court is convinced that the jury is hopelessly hung will the court accept that outcome and declare a mistrial.

The government will then have to decide whether to retry the defendant. A mistrial is not an acquittal, but it's better than a conviction.

Jurors are not always informed about what happens in cases of disagreement in the jury room. You understand that there is light at the end of the tunnel even if the jury hangs, but many of your peers don't. This knowledge is power. If you are the lone nullifier, you have little chance of winning the other 11 (or five) people over to your point of view, except for this: They want to

Twelve Angry Men, Silver Screen Collection/Getty

Nullifying illegitimate laws is easier when you understand the game that judges and attorneys are playing.

go home; they may not know whether that will happen if there is no agreement; and they are probably not as heavily invested in convicting the defendant as you are in preventing an unjust result. Those three factors give you a chance of participating in an acquittal instead of just a hung jury.

You are unlikely to get there by launching into a disquisition on the history of jury nullification in Anglo-American jurisprudence. Jurors swear to render "a true verdict according to the law and the evidence." You and I know that someone who nullifies a bad statute in order to acquit is not violating this oath—you have pledged to rule according to "the law," which includes the power to nullify. But because judges and prosecutors deny that, you may be making needless trouble for yourself by justifying your verdict in nullification terms. Your fellow jurors could complain to the judge, who will tell them nullification is *not* the law, thereby setting them more firmly against you. Depending on her level of legal ignorance, your judge also might take other action against you, such as removing you from the jury or holding you in contempt.

Because your verdict is your own personal moral judgment, you have no obligation to explain or justify it to anyone. But if you want to see the defendant acquitted, you need to give your fellow jurors some face-saving justification for moving from "guilty" to "not guilty."

Reasonable doubt is a good place to start, because it is a nebulous standard: A smart person can always find a doubt, and she can usually, if she wants to, find some rationalization for it—a reason that it is reasonable—as well. During the trial, the defense lawyer should have given you ammunition for convincing those of your peers who are inclined to convict that there is reasonable doubt in the case.

If you show a steadfast dedication to your position and you can give the other jurors some plausible reason to doubt the prosecution's case, you might just be able to turn your one vote into two, two into four, and so forth—it gets easier as you have more people on your side—until finally you've turned a hung jury into an acquittal. ◉

MARK BENNETT is a criminal defense and free-speech lawyer in Houston and a blogger at defendingpeople.com.

The Great Escape

IF YOU CAN'T AVOID GETTING INTO TROUBLE, KNOWING HOW TO GET OUT OF HANDCUFFS CAN'T HURT.

J.D. TUCCILLE

FACE SCREWED UP in concentration, my son, Anthony, turned the bobby pin. At the sound of *click* he smiled. Spinning the bobby pin in the opposite direction, clockwise now, he probed a bit, and the arm of the handcuffs slid open.

"Whoa, cool," he said.

"Yeah," I answered. "Now, let's try shimming the pawl."

That I know a few tricks for getting out of handcuffs is probably less surprising than how I learned those skills. After all, my family has some experience with shackles of various sorts. One of my father's earlier memories of his old man was seeing the latter peering through the barred rear window of a paddy wagon. Then his turn came. Jails on three continents provided unwelcome (though temporary) accommodations to my dad once he achieved his own adulthood. Things get more interesting when you include extended family, several of whom have been hosted at state expense and others of whom should have been.

So of course I learned how to open handcuffs.

The learning process was innocent, however. When I was a kid, my grandmother gave me a toy cop kit—cap pistol, badge, billy club, and handcuffs. In retrospect, the cuffs might well have been pumped out by the same company that sold the real deal to police departments. They worked the same way. There was no safety lever or button to release the lock, as would be absolutely mandatory today. There were just cuffs made from

Kuzmik_A/iStock

low-bid metal and a set of keys.

I lost the keys—and discovered this after I'd cuffed myself.

Necessity being the mother of channeling Houdini, I tried several improvised tools before settling on one of my mother's bobby pins. I bent the end a bit, probed the lock, and eventually got it to release. Then I took a closer look at the mechanism that had imprisoned me just moments before. It looked like teeth held the arm in place, and maybe the flat end of the bobby pin could slide between those teeth…Yes, it did—and the arm slid free again.

I didn't know it, but I'd just discovered "shimming."

Handcuffed people today who wish to adjust their situations are no longer left to their own devices as I was in that awkward childhood moment. We now have instructional videos on YouTube and teaching tools sold by online vendors. You can even buy escape and evasion kits from companies presenting helpful how-tos on their websites. If a neglectful kidnapper or forgetful lover leaves you chained within reach of your smartphone, you have a fair chance of figuring out how to resolve your dilemma through the world of electronic information (or calling for help, I guess, but why take the lazy way out?).

Still, who wants to leave their kid to figure things out on the internet? That's just irresponsible. Instead, I bought a practice cuff with one clear plastic side that lets you see the workings, the better to teach my son to escape from it.

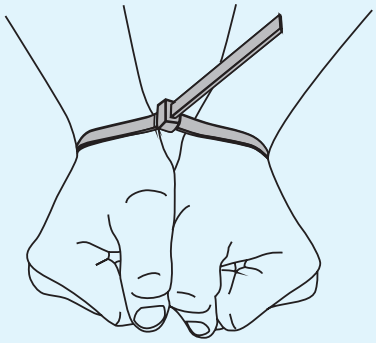
Like real handcuffs, the practice cuff also has double pawls—two sets of teeth—which are intended to defeat narrow shims like bobby pins by keeping one set engaged even if the other is lifted. Being able to see inside the mechanism let Anthony know why it was so important to run the shim right down the middle between the teeth and the arm, to get both sets of pawls. You can use wider shims, like a piece of coping saw blade, which is also handy for cutting those plastic zip cuffs. But I think it's important to start with the basics, like making use of found tools.

Included in Anthony's lessons were warnings that popping a pair of cuffs once doesn't make him Jack Bauer. Anybody restraining him—no matter which side of the law he's on—is likely to know that handcuffs are intended to be more of an inconvenience than a portable Alcatraz. They'll probably keep their prisoner under observation or otherwise try to prevent escape attempts. There are also more modern restraints that are much harder to defeat via the skills I've passed on to him.

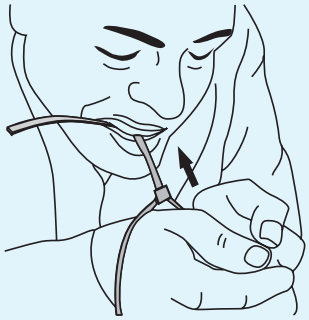
But life is about percentages. It's certainly better to have a little knowledge in reserve than to find yourself in an unpleasant situation and realize there's not much you can do about it. Besides, it's fun to learn. ◉

Contributing Editor J.D. TUCCILLE writes from Arizona.

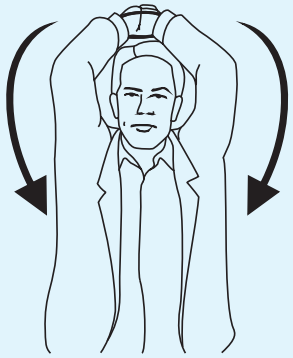
HOW TO BREAK OUT OF ZIP TIE CUFFS*



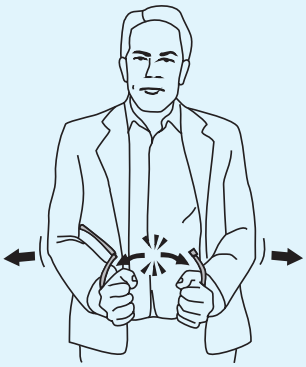
1. Make fists with both hands, palms facing each other. Ensure the locking mechanism is between them.



2. Pull on the zip tie's tail with your teeth, tightening it as much as possible.



3. Raise your hands above your head. You're going to use gravity to help you bust open the locking mechanism.



4. In one swift, powerful motion, bring your arms down into your midriff, forcing your elbows to sweep down, back, and out. This maximizes the pressure on the zip tie, which should be enough to break it.

5. The act of forcing your elbows outward should push your shoulder blades back and toward each other.

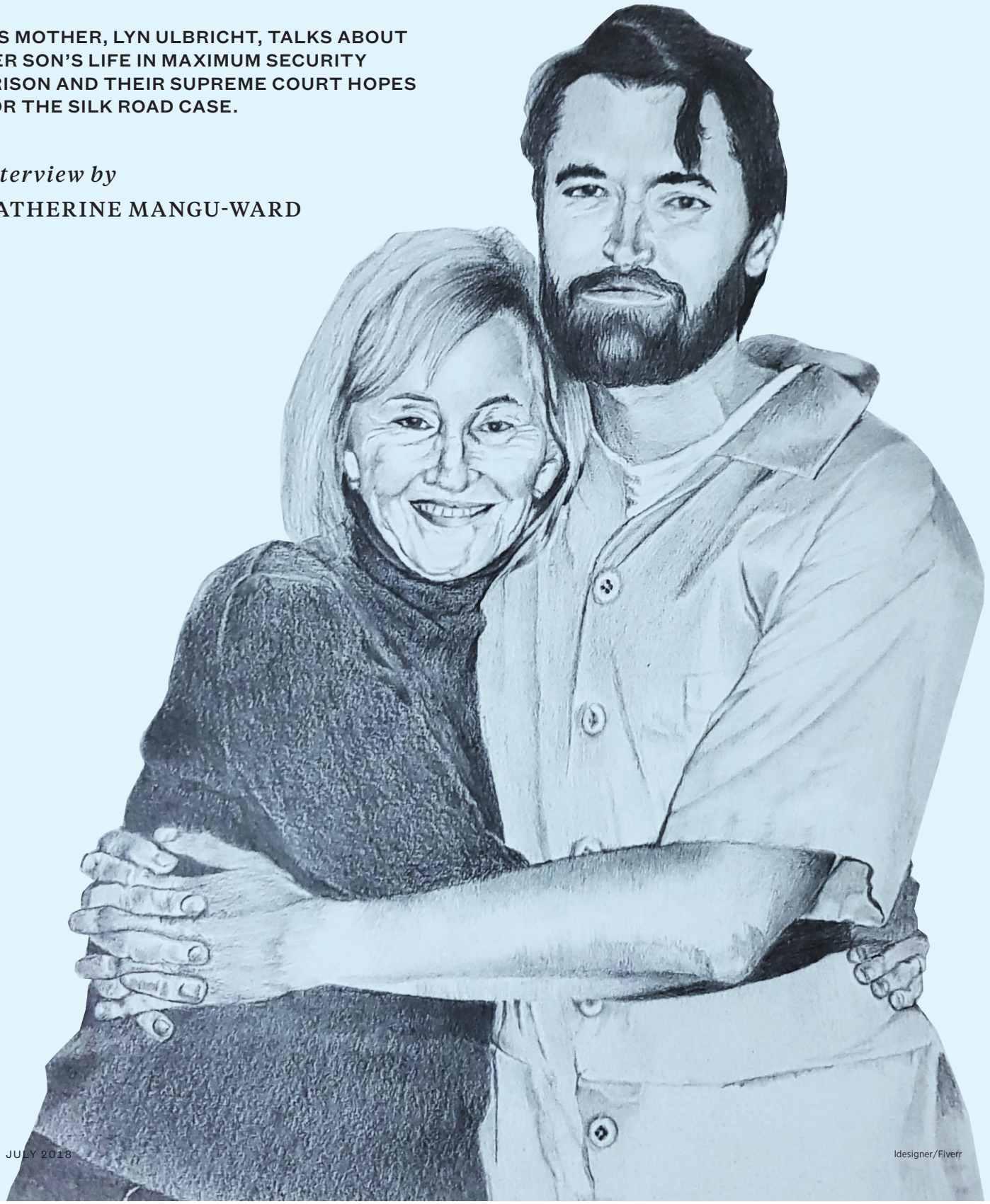
*Note: This technique can break through standard zip ties rated at roughly 50–120 pounds of tensile strength. You'll want to think twice before trying it on the extra-thick, heavy-duty kind often employed by cops. Our testers all failed to get out of 9 mm–wide 200-pound zip ties by following these directions.

pgurido/fiverr

Ross Ulbricht Is Serving a Double Life Sentence

HIS MOTHER, LYN ULBRICHT, TALKS ABOUT HER SON'S LIFE IN MAXIMUM SECURITY PRISON AND THEIR SUPREME COURT HOPES FOR THE SILK ROAD CASE.

interview by
KATHERINE MANGU-WARD



ldesigner/Fiverr

LYN ULBRICHT MOVED to Colorado last year. She uprooted her life to be near her son, Ross Ulbricht, who is an inmate in a federal maximum security prison an hour outside of Colorado Springs.

Ross is serving two concurrent life sentences for his role in the founding and running of Silk Road, a dark web bazaar where users could buy and sell drugs and other illicit items, often using bitcoin. The charges against him included money laundering, computer hacking, and conspiracy to traffic narcotics. In a separate indictment, he was charged with procuring murder. Though that charge was dropped, Judge Katherine Forrest of the Southern District of New York cited it as central to her decision to go well beyond the minimum sentence of 10 years and instead imprison him for life without parole.

At his sentencing, Ross made a modest request: "I've had my youth, and I know you must take away my middle years, but please leave me my old age....Please leave a small light at the end of the tunnel." Although Forrest was not moved, the Ulbrichts hope the Supreme Court may feel differently. If their case is accepted, it could trigger a landmark decision about digital privacy and autonomy, as well as about what responsibility the creators of online tools bear for what others do with them. *Reason*'s Katherine Mangu-Ward spoke with Lyn by phone in April, shortly after she got a small piece of encouraging news from the high court about Ross' appeal.

***Reason*: Since Ross' conviction, there have been quite a few revelations about prosecutorial misconduct and other questionable practices related to his case. Can you describe what has happened?**

Lyn Ulbricht: Even pretrial, there were so many issues. For example, the government deprived Ross of bail, based partially on allegations of murder for hire, then two months later dropped those charges. And those charges were never brought to trial. He was never tried or convicted for those charges, and yet Judge Forrest used those charges to enhance a very unreasonable sentence for all nonviolent charges.

That is one of the questions that [we're bringing to the Supreme] Court: Is it constitutional for a judge to use uncharged, unproven allegations to enhance an unreasonable sentence? That deprives Ross of his jury trial rights.

By the way, there is still an indictment [on the murder-for-hire allegation] in Maryland. It's been languishing there for almost five years, unprosecuted, based on evidence supplied by Carl Mark Force, a corrupt [Drug Enforcement Administration] agent who's now in prison.

That was another one of the things that was a huge issue: The existence of this corrupt agent was precluded from trial. The jury was not allowed to know about him or another corrupt agent who was working for the [National Security Agency] and the Secret Service at the time, Shaun Bridges. The defense didn't even know about his existence until after trial.

So this was not allowed to be known to the jury. And it seems to me that that could have easily led to casting a reasonable doubt on Ross' guilt. These people not only stole over a million dollars [from Silk Road] using their access as investigators, but they had the ability to act as Dread Pirate Roberts, the pseudonym of whoever was running the site. They could change passwords, PIN numbers, keys, write things in chats—change evidence, essentially. And this was not permitted to be known to the jury.

Our readers' ears might perk up when they hear that there was an NSA component of this, since it's not really about national security.

That part was brought up by the defense before trial, and the government never denied it. They simply mocked the defense. [The DEA's Force] said, "Oh, he's bringing up this crazy stuff about the NSA." This was around the FBI investigator Christopher Tarbell's testimony under oath about how he found the Silk Road server, which experts worldwide basically called a lie. It was gibberish, according to them. In fact, [cybersecurity expert] Robert Graham even said, "We think it was the NSA."

And this is all illegal. I think your readers probably know that, but the NSA investigating and using spying surveillance against U.S. citizens is illegal. When [*Reason*'s] Nick Gillespie interviewed [NSA whistleblower] Edward Snowden at Liberty Forum, he asked about Ross: "Can we assume that the NSA was involved?" And Snowden simply said, "Yes," and later said it was unthinkable they weren't.

Well, a few weeks ago it came out that there are classified documents from Edward Snowden showing that the NSA was tracking bitcoin users urgently. Not terrorists, mind you. Bitcoin users. And since they were illegally targeting bitcoin users, there are a lot of questions as to the validity of the investigation [against Ross] at all.

This is very, very troubling, because of course it brings up the whole question of parallel construction and what many call "intelligence laundering," where the NSA uses their extensive surveillance abilities and invasion of Americans' privacy to go after people, basically, and then turns it over to the DEA, the [Department of Justice], and the [Internal Revenue Service]. This is a real slippery slope, in my opinion, to horrible Fourth Amendment violations. And it's something that everyone should be concerned about. We're turning into a surveillance state. I don't think most people want that.

> "I want to provide to him a lifeline to the outside world, so that [the prison is] not his only reality. That's what happens to people, and then when they get out, they can't assimilate well. It's a terrible system."

What happened today with the Supreme Court?

Ross and his legal team have petitioned the Supreme Court on two very broad-reaching questions that affect a lot of people. They submitted that petition in December. And then in January, 21 groups, including Reason Foundation, joined in support of that petition in five *amicus* briefs. These are groups from both sides of the political spectrum. I think that's important to note.

We just went through the process where a batch of cases are brought into conference to evaluate whether or not the [justices] were going to take the case. If they reject it, that's very, very bad. If they are willing to take it, that's very, very good. That was on Friday, so it was kind of a nail-biter over the weekend. And on Monday we found out that at least they did not reject it. There was a list of over 200 cases they did reject, and we combed that list and Ross was not on there.

It could have been relisted—just kicked down the road to the next week. But we found out today that it was not on the list for relisting, either, which indicates very strongly that they are probably holding it, pending another important Fourth Amendment case, *Carpenter v. U.S.* [which was argued last November]. So we're happy about it. We're still in the game. Ross' case is still before the courts.

What is Ross' life like right now? I know that you visit and correspond with him frequently.

Ross has been put in a maximum security prison, which is where the Bureau of Prisons puts its most violent offenders. He's a totally peaceful guy, but he's there because they automatically put people with a life sentence in these places, whether [their crimes are] violent or not.

Ross has no record of violence. He's a first-time offender. And actually, just as an aside, I've had guards come up to me, my husband, Ross, his lawyer—not only guards, but his counselor, his case manager—and they have all said, "Ross doesn't belong in here. What's he doing in here?" It's really a dangerous place. It's full of violent people, violent gangs, and there were a couple of stabbings just last week.

Is there anything that could get him moved?

Eventually I think that you prove yourself, which of course Ross will. They love him there. He could be moved to a medium security [prison]. But that's years away. And there are violent people there, too, of course.

What is his daily schedule like? How much contact does he have with the other prisoners?

Under normal circumstances, he's in a unit and he knows a lot of the people in the unit. But a lot of times they're having lockdowns lately. That leaves him locked in his cell for days at a time. It's been, off and on, at least half the time since Thanksgiving. When he's in a normal situation, he can walk a track and look at the mountains and be outside, which is really important for Ross because he's very outdoorsy and loves nature. He can go to the law library. There's a chapel where he can go meditate or pray. They have controlled moves—they can't just wander around, but when a move comes, it's announced, and then they can move to the next thing.

He has friends. His birthday was this past month. He turned 34 in there—his fifth birthday in a cage. Some of the guys got together and paid somebody to draw a nice card for him and then put together a meal for his birthday. It was really sweet. He's had no real issues or conflict. He's well-liked, which has been true for his whole life. It applies in prison too, you know? They're people.

As someone who's in there for a different reason than many of the others, do his fellow inmates find him a curiosity?

They know everything about everybody in there. They're well aware of Ross' notoriety, and they know he's a peaceful guy. Actually, there are other nonviolent people. A good friend of his, Tony, is doing a life sentence for marijuana. He's already served 13 years, and the federal prison happens to be in Colorado, where it's legal. That's insane, OK?

There's another good friend of his, Jose, who is in there because of the three-strikes law—thank you, Bill Clinton. One of his three strikes was residual cocaine on a dollar bill years ago, and he's got a life sentence. Ross says he's such a sweet person. Not everyone in there is dangerous or violent. The guy he shares his cell with isn't, luckily. But that said, there are gangs.

[The other inmates] know who Ross is. He passes *Reason* around, and they ask him about bitcoin—they think he's the expert about things like that.

What kind of person would you have expected to find in a maximum security prison before this happened, and what do you think about the people who are his friends now?

Sometimes I say, "Ross, I worked all your life for you to have a good peer group and good influences, and now you're friends with gang leaders." He's like, "Mom, gang leaders are people too." That's his thing. And he said he hasn't met one person who's truly evil in there. He said, look, some people made very bad decisions, but a lot of it has to do with the drug war. Of course there are some people you probably wouldn't want to live next door to. I'm not for everyone getting out of prison. But we have the technology to put ankle bracelets on people, let them go home to their families and their children. I think we should do a lot more of that.

What's your best-case scenario, going forward?

I'd like to get to the point where Ross could have a new trial, a fair trial, one that brought everything forward and he would be exonerated and free. That's our goal, for Ross to be able to come out and have a life. The thing is, you'd love Ross. He's not going to be somebody who's a threat in any way, and I know that he would never even come close to crossing the line into breaking the law again. He's not that stupid, frankly. He's a fast learner.

Walk me through what happens next, legally. A lot of people seem to think that if you win at the Supreme Court, everything gets magically resolved. But it's a lot messier than that, right?

Understanding that I'm not a lawyer: Let's say they reverse *Carpenter*, meaning that the previous ruling from 1979 allowing the government to surveil us without a warrant is reversed. Then they would remand [our case] and return it to the appellate courts. Ross would be back in New York in front of the 2nd Circuit, but with guidance from the Supreme Court saying, "No, this was not done properly. This needs to be re-evaluated."

Then I would hope that they would say we'd have a retrial. At the least, I would hope and pray for a resentencing. A few people say, "Oh yeah, he deserves life." I don't think they understand what life is. I don't think they understand that what we're doing to people is torturing them and their families. Most people that I have talked to, though, say that even if Ross is guilty of everything—which I don't believe—double life is just draconian. It's part of a trend that's very alarming in our country. Life sentences have quintupled since the '80s. There are 17,000 or so people serving life who are nonviolent.

One of the reasons I have moved is to be close to Ross. I want to provide to him a lifeline to the outside world, so that [the prison is] not his only reality. That's what happens to people, and then when they get out, they can't assimilate well. It's a terrible system.

How do communications work? You can visit him in person at certain times. Is that the only way you interact?

Most of the inmates have email privileges. They do not allow Ross to have email privileges, because his is an internet crime, or something. But violent gang leaders, who have nationwide networks, they have email privileges. He gets 300 phone minutes a month. He can call us. We can't contact him.

I, and of course his father and our family and some friends, have gotten on a list to visit. You have to go through a background check and all that. In this prison, it's three days a week for five or six hours a day, so I've gotten to have a lot of time with Ross. We're lucky, you know? We have an internet business, so I can do that.

But most people can't, right?

Most people can't. I don't have a small child in school. It's very hard on families. When you see the kids in there, being torn from their fathers after the visit's over and crying, wounded, really harmed by this, it's hard to forget. It's a terrible thing what we're doing to families.

People say prison food is itself a punishment. They say it as a joke, but of course it's not even remotely funny.

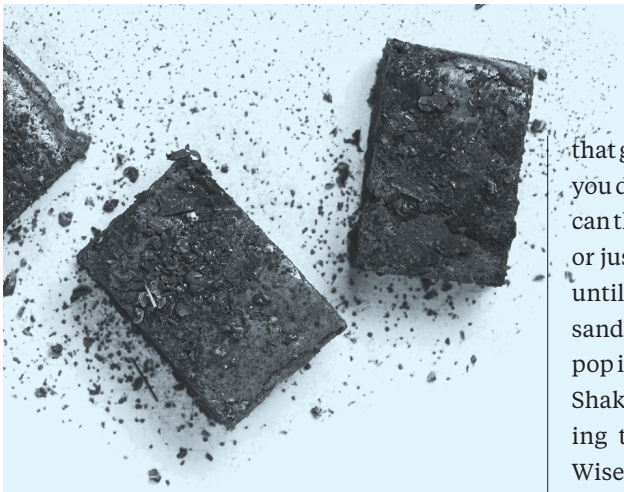
I wouldn't say that's a joke. It's certainly nothing you would order in a restaurant, let's just put it that way. Sometimes it's OK, but Ross a lot of times buys food in the commissary and makes his own food. He's doing the keto diet and the keto fasting when he can, and he's staying healthy. But yeah, I mean, prison food is pretty substandard.

Has prison changed Ross?

One of the things about prison that's the most insidious—and Ross and I were talking about this just this past weekend—is how demeaning it is. How you have a loss of dignity as a human being is really intrinsic to the whole thing. Ross says one time he was referred to as "freight." A guard into his radio was saying, "Got freight here coming up." And Ross is like, "Oh, I'm freight now?" Or they say, "We've got some bodies," or they're a number. They're stripped of their dignity as an individual.

Ross hasn't lost his dignity. He's very strong mentally and emotionally. He's reading the Stoics, he meditates, he's a spiritual person. He's staying strong, but it's very tough to keep that sense of who you are. I think people ultimately can be crushed by that. ❶

This interview has been condensed and edited for style and clarity.



REASON'S CLASSIC POT BROWNIES

KATHERINE MANGU-WARD

THE HARDEST PART about making pot brownies is the math. When you're sitting in your kitchen looking at a jar of bud, a box of butter, and a block of chocolate, the whole project can seem daunting. Fear not: Basic arithmetic and baking skills are all you need to produce your very own edibles.

First, figure out your recipe yield. I make a recipe that produces 28 brownies. Let's say I want each brownie to have 10 mg of THC—the standard dose according to the state of Colorado. Unless you have specific information from your supplier or cause to suspect otherwise, a reasonable assumption is that your bud is about 10 percent THC. (You can determine this more scientifically by buying cheap testing tools online.) 10 mg x 10 x 28 = 2,800 mg, or about 3 grams. My preferred recipe calls for three-fourths of a cup of butter. Which means I should combine **one and a half sticks (three-fourths of a cup) of butter** with my **3 grams (a little less than an eighth of an ounce) of weed**.

But you want to get as much of that THC as possible from the plant material into the butter. After a semiscientific exploration of various techniques, here's my recommendation, inspired by the work of cannabinoid scientist Tamar Wise as described in *High Times*.

You'll need to toast your cannabis. The fancy term for this is decarboxylation, which converts THCa into THC, the stuff that gets you high. Grind up your pot. If you don't have a dedicated grinder, you can throw it into a small food processor, or just break it apart with your fingers until it is roughly the texture of coarse sand. Spread it on a baking sheet and pop it in a 240-degree oven for an hour. Shake the pan a couple of times during that period to prevent burning. Wise recommends lightly spraying the toasted weed with Everclear when it comes out of the oven to break down the cellulose and maximize the release of THC, but this step is optional.

Next, infuse the butter. You can do this in a slow cooker set to low or in a small, heavy-bottomed saucepan on a burner on the lowest available setting. Combine your ground cannabis and your butter, then let the mixture cook over very low heat for a long time—at least three hours, but a full six hours is better. Stir occasionally. Strain the resulting mixture through cheesecloth, squeezing the excess butter from the spent greens.

I live in D.C., where this is a legal activity, but note that your house will smell very distinctively of marijuana during this process, so don't imagine you can do it stealthily.

If you have gone to all the trouble to produce your own cannabis butter, I strongly urge you not to waste it by throwing it into a boxed mix. Especially not when the best brownie recipe of all time is so easy: Baker's One-Bowl Brownies lend themselves particularly nicely to this preparation, since the recipe begins with warm melted butter, which is exactly what you will have once you are done.

Simply add **4 ounces of chopped unsweetened baking chocolate** to your **three-fourths of a cup of hot cannabutter** and stir until the chocolate is melted. If the butter isn't hot enough to melt all of the chocolate, pop it in the microwave for 30-second intervals until combined. Then add **2 cups of sugar**, **3 eggs**, and **2 teaspoons of vanilla**. Stir to combine, then add **1 cup of flour** and stir again. Pour the batter into a foil-lined and greased 13x9 pan and bake for 30 minutes at 350 degrees. The brownies should be just barely set in the middle when you take them out. They will firm up as they cool. Cut the resulting batch into 28 brownies.

KATHERINE MANGU-WARD is editor in chief of *Reason*.

SMOKING NOT YOUR STYLE? TRY A CANNABIS COCKTAIL.

PETER SUDERMAN

IN CALIFORNIA AND other states that have legalized marijuana for recreational use, you can now sidle up to a bar and sip something sold as a pot cocktail. These drinks tend to look a lot like the Instagram-friendly classic cocktails—think of the old fashioned, the daiquiri, and the Negroni—that have sprung up at establishments around the country, except that they are infused with cannabis. Just don't expect any of them to get you truly high.

Even in places where both pot and alcohol are legal to consume, there are legal barriers that typically prevent bars and restaurants from serving anything with THC, marijuana's main psychoactive ingredient. Instead, bartenders

serving pot cocktails infuse their drinks with cannabidiol (CBD), an oil extracted from hemp. CBD delivers a calming "body high" that goes well with alcohol but leaves your mind alone.

That doesn't mean real pot cocktails are impossible to come by. You just have to make them at home.

Infusing weed into cocktails works like infusing any other herb or spice: You can put it into your booze directly or make it part of another cocktail ingredient, such as syrups, shrubs, or bitters. Once you've created a pot-infused element, you mix it into a cocktail as you normally would—with the provisos that the taste and smell will be subtly (or in some cases radically) different, and that you should probably label the infused bottle carefully.

Balanced well, a pot infusion adds a grassy, herbal complexity to the drink, as well as an extra layer of chemically aided comfort and relaxation.

To make infused simple syrup: Start by decarboxylating the ground weed (as described in the brownie recipe), then wrap it in a cheesecloth pouch. Heat that pouch on the stove with 12 ounces of water and 12 ounces of sugar until the sugar has completely dissolved into the water. Let all the ingredients simmer on a low burner for an hour or so, then pull out the pouch, and, after it cools, pour the remaining syrup into a plastic storage container with a lid. (You can store this in your refrigerator for up to a month.)

Congratulations! You've made pot-infused simple syrup, which means you can now make pot-infused old fashioneds, sazeracs, and many other drinks.

To make infused alcohol: Infusing pot directly into alcohol is even easier. Take about a quarter-ounce of marijuana, gently grind it, then drop it into a mason jar with 16 ounces of booze. Leave it in a cool, dark location for anywhere from three days to a month. At the end, strain out the pot using cheesecloth and store the liquor in a fresh jar.

Pot-infused spirits have a vegetal, spice-rack quality to both the nose and the tongue. It's a little like sage, thyme, or arugula, which means it goes especially well with funky sours and bitter drinks, such as the underappreciated "old pal," a rye-based variation on the Negroni.

PETER SUDERMAN is managing editor at reason.com.

OLD FASHIONED

2 dashes Angostura bitters
¼ ounce pot-infused simple syrup
2 ounces uninfused bourbon
Stir all ingredients over ice 40–50 times, then strain into a double rocks glass over a 2x2-inch ice cube. Garnish with an orange twist.

OLD PAL

2 dashes Peychaud's bitters
1 ounce Cynar
1 ounce sweet vermouth (Carpano Antica or Dolin)
1 ¼ ounces pot-infused rye
Stir all ingredients over ice 40–50 times, then strain into a double rocks glass over a 2x2-inch ice cube. Garnish with a lemon twist.

A word on dosing: Pot infusions are an inexact science, and everyone reacts to marijuana differently. Consider starting with half a brownie; 5 mg is the generally accepted "rookie" dose for edibles. You can achieve the same effect by simply replacing half the cannabutter with regular butter. Similarly, don't over-infuse your alcohol. In the beginning, it's also smart to split the liquor in a recipe between infused and uninfused booze. In an "old pal," for example, you might use just a fourth of an ounce of pot-infused rye plus one ounce of unaltered rye. Always be cautious when mixing alcohol and marijuana. Basically, don't overdo it.

PRISON HOOCH
a.k.a. pruno, toilet wine, raisin jack

Ingredients:
- 10 peeled oranges
- one 8-ounce bowl of fruit cocktail
- 16 ounces of warm water
- 40–60 cubes of white sugar
- 6 teaspoons of ketchup

Time: 7–8 days, but if you're making this you've probably got nothing but time.

1. Squeeze the fruit into a large plastic bag, puree with your fists, add warm water, and seal.
2. Heat bag under hot running water for 15 minutes, wrap in a towel, and store.
3. The next day, run the bag under warm (not hot) water for 15 minutes. Add sugar and ketchup. Wrap and store.
4. Reheat daily by running under warm water for 15 minutes. (If the bag gets cold, the yeast will die.)
5. The bag will bloat from carbon dioxide, a byproduct of fermentation. Once a day, open it to release the excess gas.
6. After seven to eight days, strain through a sock—preferably a clean one—and enjoy!

NOTE: The party poopers at the Centers for Disease Control and Prevention say consuming pruno is a good way to get botulism, which can be fatal.

—C.J. CIARAMELLA

Off-Grid Survival for You and Me

A GUIDE TO MAINTAINING YOUR OWN BASIC POWER, WATER, AND SUPPLIES

J.D. TUCCILLE

MY FAMILY LIVED in a suburban garden apartment during the New York City blackout of 1977, when just two lightning strikes zipped millions of Americans back to the 19th century for roughly 24 hours. We had left the city several years earlier—fortunately, considering the rough ride urban residents had during that outage. Up the river in Tarrytown, we just congregated on the communal porch to light grills, share gossip, and bum any available candles. I can still remember the hiss of the Coleman gasoline lantern my parents had packed away with a companion camping stove. That thoughtfulness on their part allowed us luxury that those hooked on electricity flowing from far away had to do without.

When it came to unexpectedly losing some perks of modern civilization, we thrived because we were *prepared*. "Prepping" has gotten a bad name because of the loony obsessives on TV. But exhibitionist nuttiness aside, prepping is nothing more than extending to the rest of your life the same foresight that compels you to keep a spare tire and a first aid kit in your car, and maybe a puncture kit and a compressor, too.

A sensible prepper enjoys the convenience and predictability of everyday life but doesn't assume it will never be interrupted. Done right, prepping means you're not a burden on your neighbors, and can maybe help them out in the clutch—all because you did something as simple as storing fuel and a camping lantern.

The grid is amazing and wonderful. Wanting to survive off it doesn't mean you hate civilization. It means you love the conveniences of modern life enough that you've learned to provide some of them yourself.

ELECTRICITY

I'VE TAKEN MY own family even farther away from New York City, to rural Arizona. Because of that love of both civilization and independence, I'm immensely frustrated by the hurdles I've hit in trying to harness for my family's purposes that blazing ball of energy that hovers over the state. Solar power, right? It's a natural for a desert dweller. Shouldn't a nut like me, who does not want to be at the mercy of storms, lightning strikes, and low-probability disasters, have solar panels on the roof instead of a natural gas generator next to the house?

Turns out energy independence, even just for short emergencies, is a lot easier if you build from the ground up rather than retrofitting an existing structure to run off whatever juice you can self-generate. You can plan a new house to be thermally efficient, reducing heating and cooling needs, and you can equip it with appliances that sip instead of guzzle power. But if, like me, you buy a home designed to be plugged into the larger electric system, your options are limited.

Most solar installations are meant to be grid-tied and make sense only if electric utilities buy the resulting power from you. If you actually want to use the electricity *yourself*, you'll need to store it for when the sun sets. Solar panels and wind turbines are thus usually used to charge batteries, which are in turn used to power your TV and laptop. (Outside the desert, hydropower with a reliable year-round water source can free you from the need for battery storage.)

Because of that blazing ball of energy, we have *big* air conditioners in Arizona. And air conditioners, like a lot of appliances, require a starting surge to get the motor going. That surge can easily be triple the normal running load. Your battery stack must be able to accommodate that requirement for any motors you plan to plug in, and that costs money—a lot of money.

I had two companies bid on solar installations for my house. The price, including panels, batteries, inverters, and the like, came in at $30,000–$40,000. The lion's share of that amount was for the batteries.

Tax credits would've offset part of the cost. So would selling my excess power to the utility company in years to come. (This assumes the legal situation doesn't change; for now, most states require utilities to buy solar power generated by individuals.) But I wanted a backstop for occasional power outages and scarier what-if scenarios, not to explore the unlikely charms of personal bankruptcy or to dip my toes into a politically mandated market.

For a fraction of the cost of solar, therefore—about five grand plus installation, with fuel costs varying depending on market prices and how often the local grid chokes—I installed a 22-kW natural gas generator that runs *everything* in my house. We still have to rely on the flow of fuel, but that should be fine through most storms. It's true that natural gas is pressurized by pumps that, in some areas, rely on electricity (though in other places they're also gas-driven). Gas also moves through aging pipes that can be vulnerable to such disruptions as large storms, earthquakes, and, according to a March 2017 report in the *Oil and Gas, Natural Resources, and Energy Journal*, cyberattacks.

But our backup has already seen us, our refrigerated goods, and our well pump through several outages. Yes, and the air conditioner, too.

When choosing a generator, "match your power needs to the size of the generator you buy," *Consumer Reports* advises. My parents picked an 8-kW standby generator that has kept lights and sump pump going through power outages as long as a week. But when a nasty tropical storm returned their D.C.-area community to the swampy conditions whence it emerged, they said they wished they'd picked a machine with enough capacity to run the A/C and keep the house a tad more habitable. (Running grid power to the nation's capital was a mistake to begin with, if you ask me. Climate control allows riffraff of undersecretarial depravity to skulk in the vicinity year-round.)

I do have a folding solar panel and lithium battery for juicing up various gadgets. It travels with me in the car and—if I'm in the mood to be connected—when I hit the trails. Solar definitely still has its uses, and I'm planning now to harness it to add a backup to my house's backup. If I rein in expectations and accept a solar setup that can power just the necessities, such as a refrigerator, some lights, and a few small appliances, the whole thing can be kept to a reasonable size and price.

As in most areas of life, there's no one-size-fits-all solution. Plenty of people might want to go full-hog for generating their own power, making all the necessary adjustments to their homes to do so. Others think I'm nuts for worrying about a power backup at all when cheap electricity is almost always a switch-flip away. But my approach gives me peace of mind to offset the risks of our occasionally shaky power grid. All it takes is a generator rumbling, barely audibly, next to the house.

WATER

MAN CANNOT LIVE by electricity alone. Especially in the parched desert, where the water level in your well is far enough below the surface that you start to wonder if you've drilled into the communal Jacuzzi of the mole people, the wet stuff rightly takes up major space in your brain. It rains, blessedly, even in Arizona, so I've learned to tap my rain gutters and store the proceeds for use in the garden and as a backup to the well—important, since I can only run the pump if the grid is up or the generator is running.

Unlike some states, Arizona actively encourages the harvesting of rainwater—the University of Arizona even publishes a guide on how to do it, with plans that range from just sloping your driveway toward a garden that's been landscaped to hold fluids to sophisticated schemes including underground storage tanks and attached irrigation systems. A PDF version of the guide is distributed by the state Department of Water Resources.

Across the dry West, water rights are generally held separately from land rights, leading to some odd situations where property owners have limited or no access to liquid they can see and feel. But even restrictive Colorado now allows homeowners to install two rain barrels of up to 110 gallons' capacity. (You'll have to hide any extra barrels out of sight of snoopy neighbors.)

Several times over the years, my wife and I have stayed at a bed and breakfast built as a DIY project. The owner connected the structure's gutters, as well as grey water outflow from sinks, dishwashers, bathtubs, and the like, to an underground cistern of substantial size. The stored water is used for irrigation as well as limited household purposes, such as flushing toilets. The B&B is in a jurisdiction that allows for rainfall harvesting and grey water recycling but restricts their use. The owner may not have been excessively rigid in abiding by those rules, so I'll refrain from identifying the place. The setup, however, is an impressive example of maximizing your return on the available liquid in a parched environment.

Most folks aren't building homes from the ground up with such sophisticated water harvesting and reuse systems in mind. For us, something less ambitious will have to serve. Still, it's easy enough to repurpose the stuff falling from the sky in an existing house without too much trouble or expense.

Barrels and kits for diverting part or all of the flow of rain gutters are easily available from a variety of sources. I ordered mine online and picked them up free of shipping charges at a local home improvement store. The barrels even come in a variety of designs, if you're not immune to the *Westworld*-y charms of wood-patterned plastic.

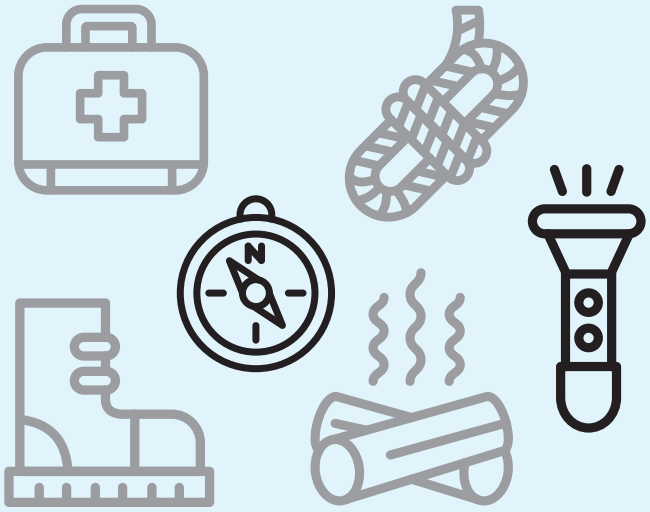
Be warned that cutting into the gutters is loud, by the way. They're basically unmelodious organ pipes that amplify the sound of your saw. I found I had to fish ear protection out of my shooting bag to get through it.

I use harvested water to irrigate my garden and some trees by the side of the house. The rain barrels have spigots that can be used to fill watering cans or be connected to hoses. They can also accommodate the sort of drip irrigation system I'm installing now, so long as you're realistic about volume and pressure, which will not be high.

One of the easier ways to make use of rain is to plant trees, shrubs, or the tomato plants with which I'm constantly struggling in basins dug into the ground. "Concave depressions planted with grass or plants serve as landscape holding areas, containing the water, increasing water penetration, and reducing flooding," the University of Arizona pamphlet advises. I came late to this lesson, but it's an effective way to slow the water

that otherwise rushes across my property during storms and into the arroyo across the road.

Like the struggle for liberty itself, my rainwater harvesting setup is a work in progress. I'm constantly tweaking it, moving components, and adding parts. However it's configured at any given time, though, it gives me a water source independent of my well. Which means I won't be completely screwed if the mole people ever get sufficiently bent out of shape to cut off the flow.



SUPPLIES

CORPSES ARE RISING from their graves, the sweet meteor of death looms over the horizon, and a fine drizzle of radioactive fallout is settling to the ground. What to do to pull through the hard times? You might have sufficient electricity and water for basic survival, but there's more to life than that.

There's only so much theoretical future disaster you can plan around without gearing your entire life to the end of the world. Unless you have a reality TV show deal, that's probably not too tempting a prospect. So let's talk about something a little less apocalyptic, like storms, floods, power outages, or a victorious Trump/Sanders ticket in 2020. You can plan ahead for these prospects without breaking the bank or your sanity. Luckily, the law doesn't put too many barriers in the way of my particular pointers for making it out alive.

The American Red Cross recommends you have three days of food and water on hand for evacuations and two weeks' worth for home use in case of an emergency. That's probably the minimum you should consider. We're backpackers, so I keep our packs loaded up with a long weekend's quantity of camping supplies, including freeze-dried meals, a water filter, clothing, shelter, sleeping bags, a stove, and the like. You can skip the stove (and the need to rotate liquid fuel) if you stick with cold meals, but you'll still want a means of making fire for warmth.

By the way, that backpack is where you're going to stick your important documents and cash supply. You are keeping them in one place, and you remember where that is, right?

Put the backpack on. Look down. Can you see your toes? Remember, if you have to evacuate, the most important survival tool is your body and whatever physical condition—and abilities—it has to offer.

Keeping two weeks of food at home isn't that hard. Just buy some extra canned goods at every trip to the market, and push the newer purchases to the back of the pantry behind food you'll eat first. For longer-term storage—how long depends on what you're planning for, but Mormons are counseled by their church to keep a three-month supply—consider No. 10 cans of freeze-dried food, which stay good for decades.

A camp stove and fuel may be your only means of making meals if power and gas are out. After Hurricane Sandy, many Long Island residents waited two weeks for the lights to come back on—and that was merciful compared to the monthslong blackout that Hurricane Maria inflicted on Puerto Rico last year.

If you're an urban apartment dweller for whom the above advice about rainwater collection isn't useful, remember that two weeks of water takes a lot of weight and volume. Bleach and food-grade blue barrels can help keep a usable supply handy. In a pinch, the bathtub and collapsible containers that can be filled from the tap as a nasty storm is rolling in may be your best bet.

Filters and chemical treatment are handy in case you have to resort to water sources of unknown purity. With proper treatment (and by necessity) I've drunk from cattle tanks that more closely resembled cesspools than springs. I'm not saying I liked it, but I lived to tell the tale.

I would skip those hand-cranked radios and lanterns that certain vendors have been peddling for years in favor of a double-handful of rechargeable batteries that fit your existing devices. Bundle 'em up with a folding solar panel that can connect to a USB-equipped charger, plus an external lithium battery pack. This way you have some widgets that you can actually use, for camping and road-tripping, say, and not just in case of cataclysm.

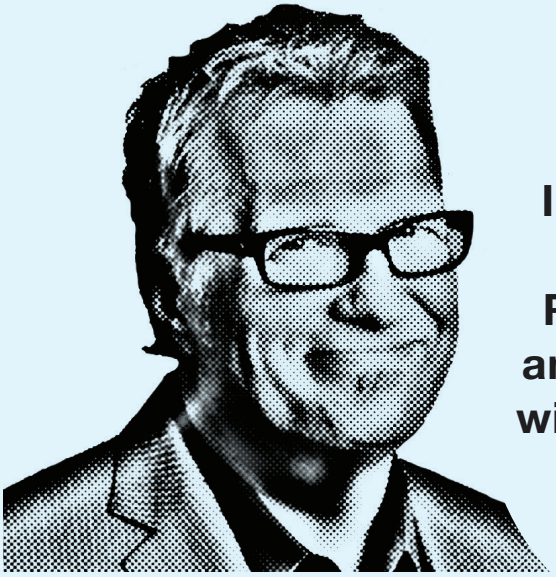
If you're not already a gun owner, consider at least a pistol and rifle in commonly available .22 LR. That's a caliber useful in a multitude of situations, from bagging small game to (in a pinch) self-defense. The ammunition is cheap and portable; survivors will probably count it as money after the radioactive undead rise from their graves; and the same box of rounds will feed both firearms. You might want to mind the specific laws of your locality about weapon possession, carrying, and registration. Then again, thinking about your family's survival when worst comes to worst, you might not. ®

Contributing Editor J.D. TUCCILLE writes from Arizona.

vasabii/bergserg/iStock

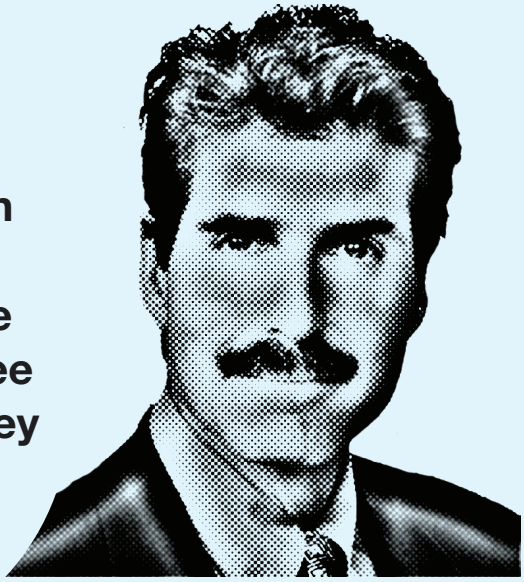
reason FOUNDATION

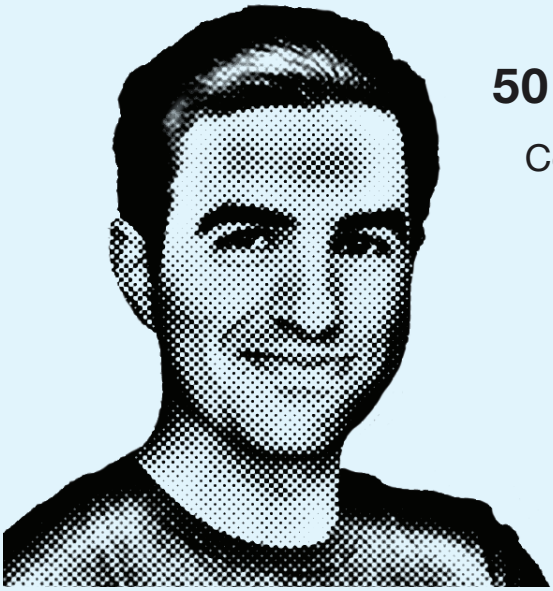
50 years



“I never thought I was a libertarian until I picked up Reason magazine and realized I agree with everything they had printed.”

Drew Carey





50 Years of Liberty!

Come to Reason’s 50th Anniversary Gala
November 3rd, 2018
Register today at
reason.org/events

CELEBRATING 50 YEARS OF REASON PEOPLE AND IDEAS

Reason TV Stars: Drew Carey, John Stossel, Kennedy, Remy

Outlaw Mags

***REASON* REVIEWS CONTROVERSIAL AND OFT-CENSORED PUBLICATIONS.**

C.J. CIARAMELLA AND CHRISTIAN BRITSCHGI

PRISON LEGAL NEWS

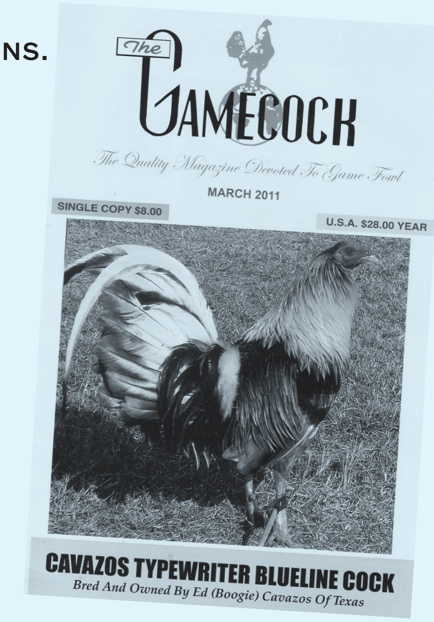
UH OH—LOOKS LIKE you've landed behind bars. You should pick up a copy of *Prison Legal News*. This monthly magazine, the oldest continual publication written by and for inmates, is an indispensable resource on prison issues, prisoner rights, and the ins and outs of civil litigation in a system seemingly designed to keep prisoners from winning their freedom.

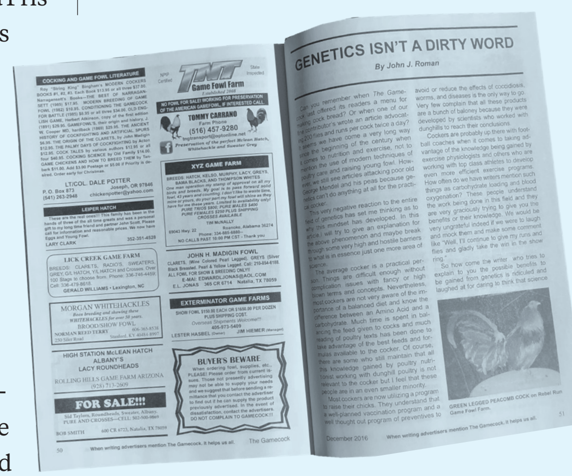
America's 2 million incarcerated people suffer inhumane conditions and civil liberties abuses that are mostly invisible to the rest of the country. Inmates have little recourse and even fewer sources of helpful, relevant information.

Of course, many prison administrators prefer that their inmates not be civil litigation experts. As a result, *Prison Legal News* is possibly the most frequently banned magazine in the United States. It has brought countless First Amendment challenges, filed public records lawsuits, and submitted friend of the court briefs against censorious prisons in 29 states to get its issues into inmates' hands.

Even for those not in the clink it's a magazine worth reading, if only to absorb the magnitude of the problem. A sample of headlines from the publication's April issue: "California: Mentally Ill Jail Prisoner Dies after Two Days in Restraint Chair; $5 Million Settlement," "Louisiana Prison Officials Sued for Trying to Block Investigation into Abuse of Disabled Prisoners," and "Florida KKK Guards Convicted in Plot to Kill Former Prisoner."

It's a hell of a system, and *Prison Legal News* is one of the few publications dedicated to documenting it.





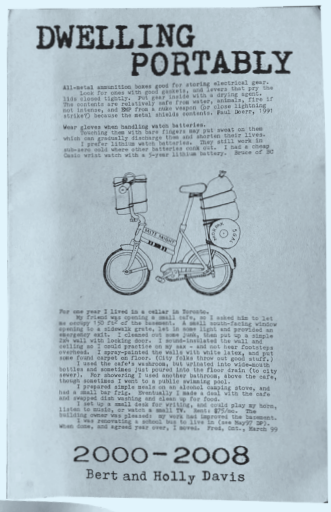
THE GAMECOCK

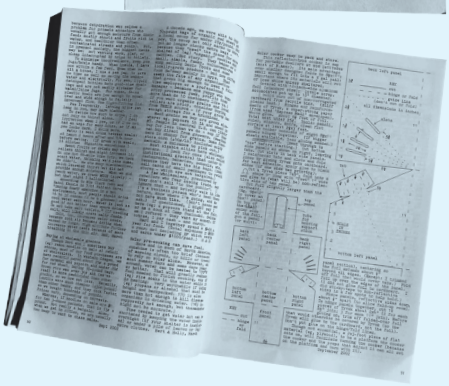
***THE GAMECOCK* IS** not for casual cockers. Everything about the magazine suggests it's geared toward diehard participants of the now illicit sport of cockfighting.

The magazine's cover is decidedly understated, with most issues featuring only the title and the profile of a ring-ready rooster on a cream-colored background. Flip it open to find black-and-white photos alongside content geared not toward mass appeal but rather toward serving expert practitioners of this black art. That includes features about fighting birds, with descriptions listing the breed, price, and contact information for the seller. There are ads for performance-enhancing drugs guaranteed to improve fight performance by 10 percent as well as obits for dearly departed cockers (that is, the human owners, not the birds).

Sadly, *The Gamecock* is hard to come by these days. Lawsuits from animal rights groups got it pulled off Amazon, and in 2007 Congress passed a law prohibiting websites and magazines from advertising these fine fighting fowls, essentially killing *The Gamecock*'s funding stream.

Looking at fragments of the magazine online can thus make one nostalgic for a time when watching two birds tear each other apart in the ring was a beloved pastime and not the subject of a puritanical prohibition.



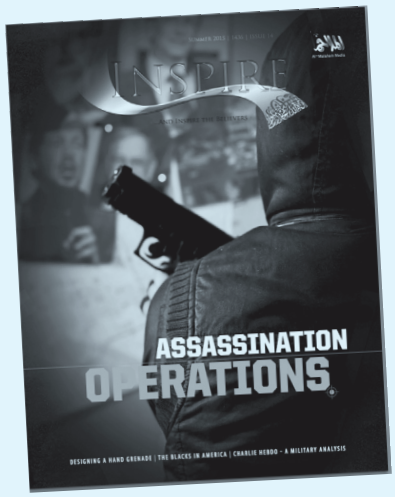


DWELLING PORTABLY

SINCE 1980, BERT and Holly Davis have been writing issues of *Dwelling Portably* from a yurt in an undisclosed location in Oregon. The 'zine offers a fascinating, idiosyncratic look into do-it-yourself homesteading and living off the grid.

Written on a manual typewriter in minuscule font (to save paper), the publication is jampacked with decades' worth of know-how and gives readers the skinny on everything from how to construct a solar water heater to the legality of dumpster diving. Want to build a $20 dugout shelter using no poles or supports? Bert and Holly have got you covered, literally.

If you're a DIY enthusiast, an aspiring urban nomad, or someone who daydreams about rejecting the trappings of modernity and just living, man, *Dwelling Portably* is your ticket to ride. Various online 'zine distros, such as Microcosm, carry collections of it. And if you can track down the current P.O. box the Davises are using, you can send them some crisp dollar bills in exchange for an issue.



INSPIRE

IN THE MINDS of many people, Al Qaeda is the embodiment of evil, and for good reason: The Islamic terrorist organization has killed a lot of innocent people.

Yet for such a homicidal bunch, the group's print magazine *Inspire* is chillingly normal. Its presentation is utterly indistinguishable from many mainstream publications found on ordinary newsstands in the West, down to the glossy pages and custom graphics. The same can be said of its format, which is a mix of features, interviews, handy how-tos, and advice columns.

Even much of the content wouldn't be out of place in some of America's more solidly left-wing magazines, provided the prose were tightened and scrubbed of its religious references. The Summer 2017 issue features articles criticizing capitalism for its heartless lack of concern for the poor and calling out the U.S. for hypocrisy when it comes to guaranteeing freedom for racial minorities. The latter is complete with a picture of the police killing Eric Garner. *Inspire* even shares a progressive enthusiasm for rail transit, referring to it as "the most modern and important means of transportation."

Of course, for all this uncomfortable normality, there is still plenty that is shockingly violent, including a step-by-step guide to derailing those "modern and important" trains and an editor's note explaining why violence against civilians is justifiable.

Aesthetic standards, it would appear, are more universal than moral ones.

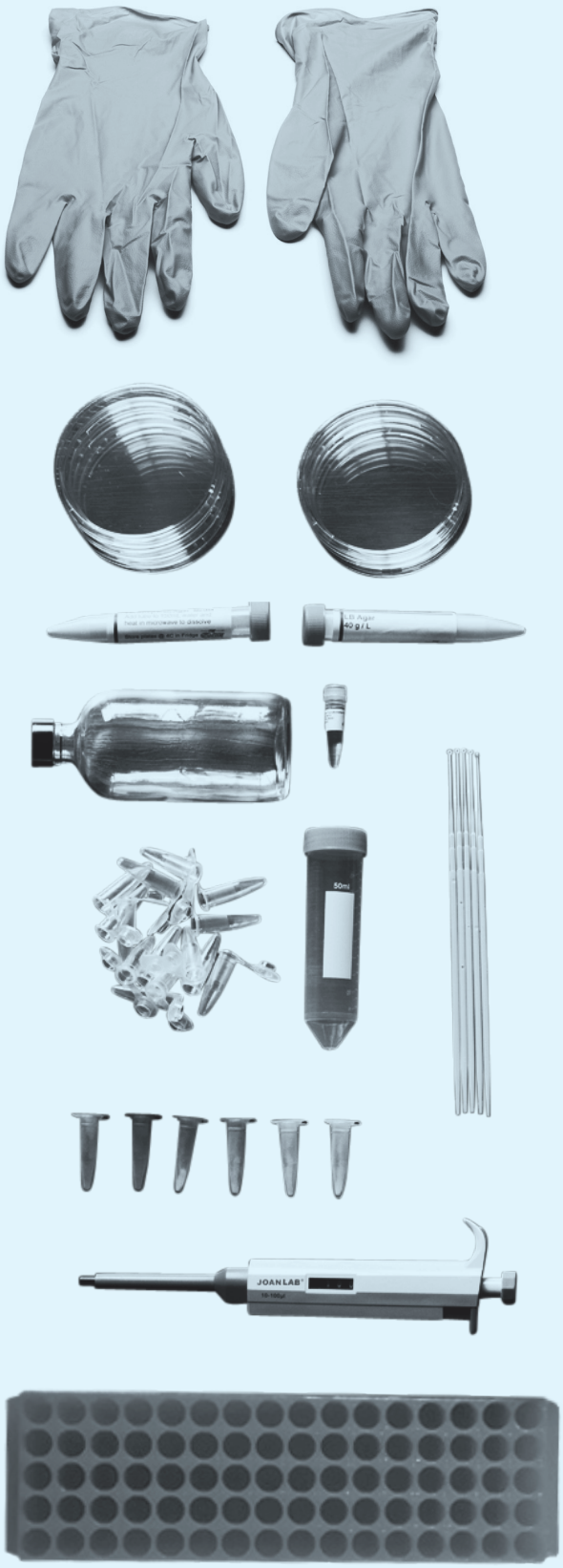
DON DIVA

***DON DIVA* HAS** been documenting gangster exploits in and out of prison since 1999. The quarterly magazine, beloved by inmates and loathed by jailers, isn't idly boasting when it refers to itself as "the original street bible."

"*Don Diva* is like the *Wall Street Journal* of gangsta lore," one inmate told the *Huffington Post*. "And being that they don't let [copies of the publication] in the pens, it's like reading a rare or lost book of the bible when someone manages to get one in."

Because of its sterling reputation among inmates, *Don Diva* regularly scoops more well-heeled publications and scores rare interviews, including one with former Detroit Mayor Kwame Kilpatrick, who is currently riding out a 28-year federal prison sentence for fraud and racketeering.

If you want the nitty gritty on who just got sentenced to hard time for hiring a hitman, thoughtful takes on the criminal justice system written from insider perspectives, or even a feature-length analysis of how "pharma bro" Martin Shkreli (who was convicted of securities fraud earlier this year) might fare behind bars, look no further than the original street bible. ●



Adventures in Home Biohacking

I MADE ANTIBIOTIC-RESISTANT E. COLI IN MY KITCHEN, AND THE WORLD DIDN'T END.

RONALD BAILEY

MY GENETK DESIGN Kits arrived in a box bearing a stylized version of Yggdrasil, the world tree in Norse mythology, with a twist of the DNA double-helix as part of its trunk. On the sides of the box, Odin's ravens, Huginn (thought) and Muninn (memory), exchange a strand of DNA. Odin had, in fact, sent me the box, and by Odin, I mean The ODIN—The Open Discovery Institute, a company that aims to make do-it-yourself genome editing easy. I was ready to start genetically editing bacteria at home.

This is possible because of CRISPR, a technology that is already revolutionizing food, medicine, and more. CRISPR comprises two key molecules. One is the Cas9 protein, an enzyme that can cut two strands of DNA at a specific location in the genome so that bits of DNA can then be added or removed. The second is a single-strand RNA that can identify and guide the protein to exactly the site in a genome that a researcher wants to engineer. The system has been likened to precise molecular scissors.

Using the handy tools sent in the kit, I was set to re-engineer some nonpathogenic E. coli in my kitchen. That might sound terrifying; surely journalists shouldn't be trusted to build superbugs. Relax. The lab-created strain provided in the kit was developed to be easy to engineer and does not live in the wild. While CRISPR holds incredible potential for in-lab and at-home genetic modification and experimentation, my efforts were strictly school science fair stuff—my modified bacteria posed no civilizational risk, and the process of creating them was fun, fascinating, and empowering.

THE CRISPR REVOLUTION began in 2012, when Jennifer Doudna of Berkeley and Emmanuelle Charpentier of Sweden's Umeå University published an article in *Science* describing how elements of a bacterial immune system could be used as a very precise gene-editing tool. In 2013, Broad Institute researcher Feng Zhang showed that CRISPR could edit genes in human cells. (A big CRISPR patent fight between Berkeley and the Broad Institute is now underway.)

Since then, there's been a flood of research into therapeutic uses of the technique. Last year, Shoukhrat Mitalipov of Oregon Health and Science University used CRISPR to correct a genetic mutation in human embryos that causes heart disease. Other

the-odin.com, APCortizasJr/iStock

researchers are working on CRISPR therapies to cure Huntington's, Parkinson's, sickle cell anemia, Duchenne muscular dystrophy, and various congenital blindnesses. Chinese physicians are already running trials in which they use CRISPR to rev up cancer patients' immune cells. This summer a trial at the University of Pennsylvania will try to use CRISPR techniques to treat multiple myeloma, sarcoma, and melanoma. Some researchers think a one-time CRISPR "vaccination" could edit a specific gene associated with cholesterol, thus lowering a patient's risk of various cardiovascular diseases.

The technology will also radically change how we grow our crops, make our foods, and curate our natural environment. With gene editing, researchers can make changes to a plant or animal's *existing* genome—a departure from the conventional genetic modification technique, which inserts useful genes taken from other creatures. As a result, many researchers and developers argue that genome editing should be much more lightly regulated than conventional genetic engineering has been.

The ODIN already sells a kit allowing home gene jockeys to brew green glowing beer. (The kit enables a user to inject a gene for a harmless green fluorescent protein derived from jellyfish into the yeast.) Researchers at the University of California have used CRISPR to edit flavor directly into yeast, so brewers no longer have to add finicky and expensive hops to make the IPAs I relish.

Plant breeders are using CRISPR to improve various crops. DuPont has a CRISPR-edited waxy corn that is resistant to drought and disease. Wang Wei of Kansas State University has edited 25 wheat genes to dramatically increase yields. A Spanish research group has edited out the wheat genes that produce the gluten proteins that bedevil folks with celiac disease. Researchers in Colombia are CRISPRing rice and cassava to make them resistant to diseases, and altering beans to make them more easily digestible.

Animal breeders have deployed CRISPR to eliminate dangerous horns on dairy cattle and to skew the production of calves toward males in order to boost beef production. The ODIN's founder, the biohacker Josiah Zayner, injected himself last October with CRISPRed DNA designed to silence the myostatin genes that regulate muscle growth. The goal was to enhance his physique by letting his muscles get larger than they otherwise would. So far he has reported no results from the experiment. But whether or not Zayner manages to use CRISPR to knock out his own myostatin genes, the technique has been used successfully to make more ham by generating extra-muscular pigs.

The technology can also be used to create "gene drives." A gene drive works by making sure that all copies of the natural gene are replaced with the engineered versions in the progeny of CRISPRed organisms. This causes a desired trait to spread rapidly through a whole population in a natural environment. It would be possible, for example, to edit resistance to the malaria parasite or the Zika virus into entire populations of mosquitoes. A gene drive could also be constructed such that only males of an undesired species are born.

In 2015, *Science* hailed CRISPR gene editing as the breakthrough of the year. It is, the magazine declared, "only slightly hyperbolic to say that if scientists can dream of a genetic manipulation, CRISPR can now make it happen." As you can see from my very incomplete review of the rapid progress being made, it is hardly hyperbolic at all.

With great power comes great responsibility, of course, and the fight over the regulation of in-lab and at-home genetic modification is raging. You may want to order a CRISPR kit soon, in case the prohibitionists win.

WITH MY WIFE'S tolerance, I stored my kit in our refrigerator and set up a gene-editing laboratory on a red towel on our kitchen counter. Thankfully, our dinner guests were too polite to mention the petri dishes streaked with bacteria or the other lab equipment spread out in the kitchen.

For those of us who are not practiced lab jockeys, the instruction booklet that accompanies the kit is a bit opaque. Fortunately, there are some online videos to show novices how to brew up agar and to pipette biochemicals into microcentrifuge tubes.

Besides the various mixing bottles and measuring tubes, the Genetk Design Kits box came with nitrile gloves, LB Agar powder on which to grow bacteria, and LB Agar powder spiked with the antibiotics streptomycin and kanamycin. Containers held the nonpathogenic E. coli, a solution of calcium chloride and polyethylene glycol (the "bacterial transformation buffer"), Cas9 plasmid, guide RNA, and template DNA for antibiotic resistance.

With help from those online videos, I made both regular and antibiotic-spiked agar and poured each mixture onto seven petri dishes, where the agar congealed. Next, I used a plastic inoculation loop to scoop some bacteria out of their bottle and streak them onto a couple of the agar dishes to grow. As a control, I also spread some onto the plates spiked with antibiotics to see if the drugs would prevent bacterial growth.

After incubating at room temperature for about 24 hours, the bacterial streaks on the regular agar plates turned white and widened. Due no doubt to my sloppy lab work and the ubiquitous presence of bacteria, several of the regular agar plates I did not streak grew nice round wild colonies as well. Nothing was seen growing on the streptomycin/kanamycin plates.

The next day, I scraped fresh bacteria off of the plates with another inoculation loop and dumped these into the tube containing the transformation buffer, a substance that basically opens up the bacteria so that the elements of the CRISPR system can sneak in to engineer the target gene.

After refrigerating the bacteria in the transformation buffer for 30 minutes, I heat-shocked them in 108-degree water—measured using a meat thermometer—for 30 seconds. Then I pipetted 500 microliters of regular agar solution into the transformation tube and let it set for four hours at room temperature.

In this way, I made two batches of genetically engineered bacteria. The genomes of E. coli consist of about 4 million DNA base pairs; the goal of this experiment was to change just one of those, which should be enough to allow the bacteria to resist the streptomycin.

What is supposed to happen next is that the Cas9 protein incorporates the guide RNA. The particular guide RNA supplied by The ODIN consists of trans-activating CRISPR RNA (tracrRNA), which binds to the Cas9 protein and links to the CRISPR RNA (crRNA), which in turn targets the DNA in the genome to be edited. In addition to the Cas9 editing system, the bacteria have been flooded with copies of template DNA that differs from the region on the gene targeted for engineering by one base pair.

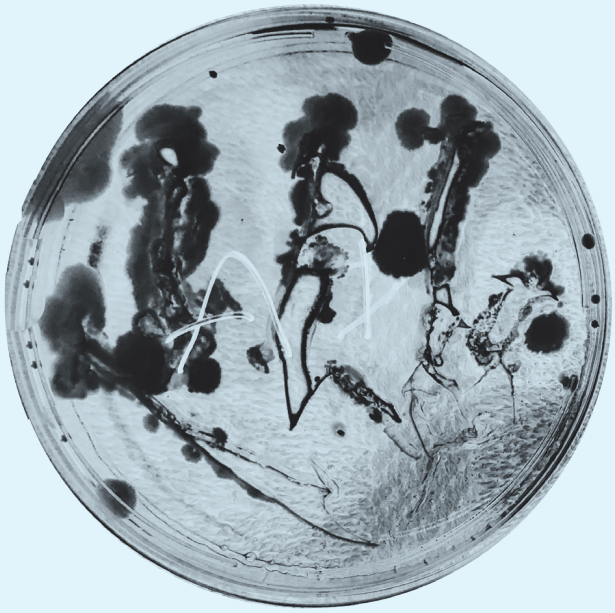
CRISPR guides the Cas9 complex to the bacteria's rpsL gene, where it makes a cut in both strands of the DNA. When such double strand breaks occur, bacteria have a natural process that seeks to repair them by searching for copies of the broken gene elsewhere in their genomes and then matching the copies.

The rpsL gene is basically a recipe that instructs cellular machinery on how to produce the S12 protein, which is crucial to the operation of ribosomes—the complex macromolecules that make and repair essential proteins in the bacteria, keeping it healthy. Streptomycin works by binding to normal S12 proteins, which disables the ribosomes' vital operation and ultimately kills the bacteria.

The DNA base pairs in the template DNA supplied by The ODIN are identical to those surrounding the cut except for the one base pair that is to be engineered. This tricks the bacteria into using the template to repair the cut made by the Cas9 protein. The only difference is that a guanine/cytosine base pair is substituted for a thymine/adenine base pair. This small change in the rpsL recipe results in a slightly reshaped version of the S12 protein, and that thwarts the antibiotic from binding to and disabling it.

If the transformation is successful, the engineered bacteria will be able to grow despite the presence of streptomycin. The last step, then, was for me to pipette 200 microliters of the (hopefully) transformed bacteria from each of my two batches onto a couple of plates containing drugged agar.

SO DID IT work? After 24 hours, I could detect no obvious growth of bacteria on the antibiotic plates from either of my two initial batches. But most of the bacteria in the 200 microliters taken from the transformation tubes and swabbed onto the petri



dish plates will in fact not have been edited. Consequently, the ones that *are* edited and *do* survive appear on the plates dosed with antibiotics as small dots, rather than the broad swipes that appear on regular, nondrugged plates.

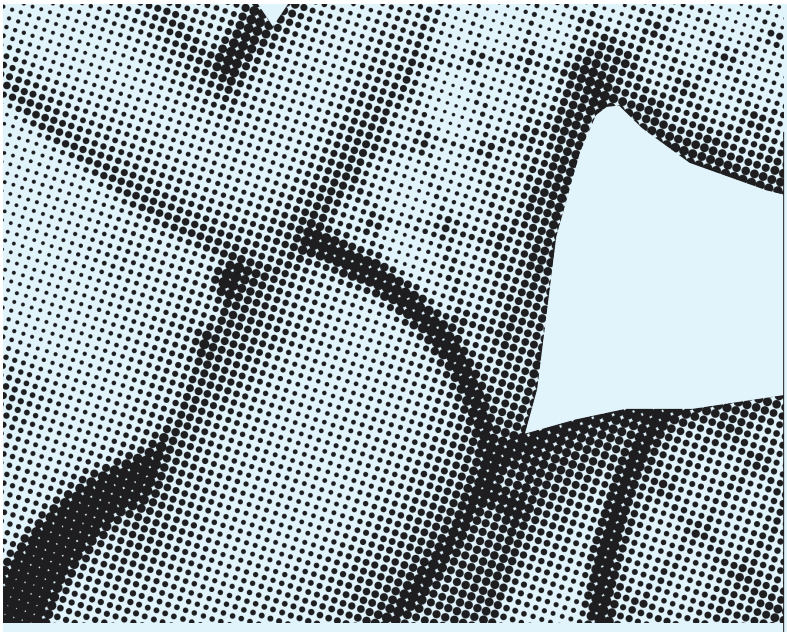
Fearing that my first two batches had failed, I whipped up a third tube and pipetted some of its bacteria onto a couple of new plates. Hoping that additional time might have worked to transform the bacteria in the first two batches, I pipetted some from those batches onto new plates as well. Finally, as a control, I pipetted bacteria from all three transformed batches onto regular agar plates, where they grew robustly.

More than 60 hours later, by squinting hard, I detected a few tiny scattered colonies on one of the antibiotic-infused plates doused with bacteria from the first transformation batch. As recommended by The ODIN—even though the E. coli I was working with is non-pathogenic—I then sterilized all the plates by dousing them with a bleach solution. While my experiment posed no danger to public health, some worry DIY CRISPRing could create deadly pandemics. But sextillions of daily *natural* experiments suggest that creating human pathogens is not that easy. Plus, vastly more researchers will be developing beneficial uses of CRISPR, including early warning diagnostics and treatments enabling us to counter any future pandemics.

The experiment was a qualified success at best. Nevertheless, DIY CRISPRing at my kitchen counter reveals just how straightforward and versatile this amazing technology is. Given the spectacular progress researchers are making toward curing diseases, enhancing plants and animals, and curating wild landscapes, it's now clear that this is CRISPR's world; we just have the good fortune to be living in it. ●

Science Correspondent RONALD BAILEY is the author of *The End of Doom: Environmental Renewal in the 21st Century* (St. Martin's).

Photo: Ronald Bailey



What to Know Before You Pay for Sex

TIPS, TRICKS, AND COMMON SENSE TO MAKE HIRING AN ESCORT A BREEZE

MAGGIE MCNEILL

IN 1948, THE noted sex researcher Alfred Kinsey reported that 69 percent of men had paid for sex at some point in their lives. The 2005 General Social Survey put the number at closer to 15 percent. The true answer is probably somewhere in between—not just because time has passed and norms have changed, but because getting people to answer such questions honestly is not always possible. Still, it's clear even from the low-end estimates that hiring a sex worker is a pretty normal thing to do. I've been an escort since January 2000, I was a stripper for two years before that, and I practiced what the literature calls "casual prostitution" going back to 1985. In those years I've seen men of all ages, from 18 to 94, and all walks of life, from a truck driver to a U.S. senator. I've made a good living at it, and so do roughly half a million other women in the United States.

Despite being a common activity, buying sexual services can be intimidating. As with all black market transactions, there is an element of risk and uncertainty caused by prohibition. Maybe you're considering buying sex but are unsure how to proceed. Or maybe you've done it in the past but are nervous in the current climate of aggressive "end demand" stings and "john shaming"—complete with names and pictures in the news. Either way, you've come to the right place: Hiring an escort is neither difficult nor dangerous as long as one exercises patience, diligence, and good manners.

Before starting, it's a good idea to have in mind what you're looking for. Is there a particular kind of person you're interested in, such as someone with certain physical characteristics or a certain educational level? Do you have a particular interest—a kink or fetish, for example—that your regular partner is unwilling or unable to fulfill? Maybe you've fantasized about being with a transgender woman, a pair of bisexual temptresses, or a lady who can really wield a whip? Are you sexually bored and looking for someone to give you the kind of bed-busting experience you've seen in porn? Or perhaps you're simply lonely and would like an interesting companion for the evening?

As long as you live in or can travel to a city of at least moderate size, it's extremely likely you'll be able to find a sex worker online who fits the bill. But to do so, you're going to need to do your research, and this is where the patience comes in. Even if you're just looking for a decently attractive gal (or guy!) to give you a good time without drama, it's still a good idea not to be in too much of a rush. Don't jump on your computer at 11 p.m. and expect to have the perfect partner at your door by midnight. Hurrying things is a good way to be disappointed, if not robbed or arrested.

Not to say there aren't escort agencies who might be able to help you in a jiffy, or that behind every goofy emoji-laden ad lurks a cop or con artist. But if you put at least as much effort into choosing an escort as you would into picking a fine restaurant or a mechanic, you'll maximize your chance of having a satisfying experience.

The seizure this year of the classified site Backpage.com by federal authorities (for alleged money laundering and facilitating prostitution) has shaken up sex-work advertising, as has the passage of a new law, the Allow States and Victims to Fight Online Sex Trafficking Act (known as FOSTA). In the wake of FOSTA—which makes it a federal crime to host digital content that promotes or facilitates prostitution and, importantly, allows web publishers and platforms to be held liable—Craigslist shut down its personals section, multiple escorting forums have closed, and some foreign websites have started blocking U.S. visitors. But there are many different places for sex professionals to advertise online, and it is possible to connect without putting you, them, or the platform operator at risk.

These websites range from the no-frills to the glossy, from the local to the international. Though I wish there were an easy, universal formula I could give you for finding such resources, there really isn't. A Google search for "escorts" and your city is not a bad jumping-off point, but be aware that not all of what comes up will be high-quality. There are quite a few scraper sites, for example, that harvest escort ads from legitimate platforms in order to draw page views but don't care whether those ads are current or even real. (I still get calls from a post I put up in Tulsa

Joanna Andreasson, mocker_bat/iStock

more than a year before I moved to Seattle in 2015.) Big names such as Eros and Slixa (both hosted outside the United States), or a review board concentrating on your geographic location, are usually a good way to start.

Notice I said "start." Once you look through the ads—and most of the good sites have them subdivided by categories, such as "mature," "GFE" ("girlfriend experience"), "tantra," and so on—and find a service provider you think you'd like to see, the next step is to do a bit *more* research. Most established professionals will link to their websites from their ads. If you don't see such a link, a search with name and city will often turn it up.

Here comes the "diligence" part: Read the provider's site, and I don't just mean skimming it for the first thing that looks like a point of contact or glancing at the pictures. I mean *read* it, especially the rates page and the contact information. Trust me, guys, there is nothing that will annoy a pro more than an email containing a bunch of questions that are answered right there on the website. When escorts get together with each other for drinks, this is one of the most common things we bitch about. On the other hand, demonstrating that you *did* read the site by following the contact instructions correctly is an excellent way to get on your provider's good side from the get-go. (This is especially true of dominatrices, in my experience.)

If you're nervous and/or picky, this is the time to look at the person's online footprint. For years, reviews were a good way to find out what kinds of experiences other clients had with the lady you're considering, but that's not as true as it once was. While many sex workers like getting reviews and will happily point you to them (and some even prefer that you consult them rather than ask questions), others dislike or distrust them. For some, including me, it's a matter of taste: Reviews can often be crass and vulgar even when they're complimentary. They are also regularly embellished to make the reviewer look more studly—so much so that the information conveyed can be…let's just say "less than accurate."

But beyond that, the review system has been undermined by bad actors from both inside and outside of the sex-work community. Unscrupulous clients use the promise of good reviews or the threat of bad ones to coerce inexperienced girls into out-of-bounds activities; unprincipled profiteers sell fake reviews to equally unprincipled escorts; and unethical prosecutors have begun to charge clients who write reviews with "facilitating prostitution." Plus, due to the aforementioned FOSTA, some sites are either closing their reviews to U.S. readers or removing them entirely.

By all means, consult the reviews if a provider has them, but also (or instead) check whether she has a blog, a Twitter account, message-board posts, pictures whose image searches lead you back to a website, and other signs this is a real person rather than a sock puppet created by cops or crooks to ensnare the unwary.

Once you've found a provider you really want to see, verified to your satisfaction that she is an established professional with a history of satisfied customers, and absorbed pertinent public info about rates, hours, etc., it's time to make contact. But be warned: Just as you wanted to know what you were getting, sex workers want to know what *they* are getting. Reach out in whatever way the website directs, and provide whatever information is requested. Don't try to get cute, and don't act pushy or overly defensive: While you may be worried about being cheated or arrested, we're worried about those things *plus* the possibility of a rough, abusive, or violent client.

Most providers will ask for references—that is, the names and contact info of other professionals you've seen. For your sake, it's best to give at least two, in case one is slow to respond or doesn't remember you. "Bambi from Backpage, I don't recall her number" ain't gonna cut it. If you have never seen a pro before, or if it's been more than a few years, be honest about that; some will turn you down without references, but others are "newbie friendly" and will screen you by other means, such as employment verification or connecting with you on a site such as LinkedIn. Don't be shy—remember, you've already verified *her*, and she has no reason to risk her reputation and business by outing you. But if you do feel the provider is asking too much, you should politely decline and find someone else; pressuring a sex worker to "make an exception" won't get you anywhere except onto a blacklist.

(There are also whitelist services that will use employment verification and/or public records to confirm you are who you claim, giving you a number or other tag by which your certification can be looked up from our end. However, they typically charge a fee, not every pro accepts them, and they're going to ask you for screening info as well. I'd advise you to look into those later, after you've decided this is something you want to do regularly.)

If you've done all that and secured an appointment, the rest can be summed up in three words: Be a gentleman. Don't haggle over price, be coy with payment, ask rude or prying questions, push boundaries, or even *think* about asking for unprotected sex. Do be prompt (which does not mean "early"), clean (that means soap, including your whole crotch region), generous (a tip or small gift is not expected, but it is definitely appreciated), and as respectful as you would be of any other businessperson. If you have to cancel, do so far in advance, and if that isn't possible, either offer to pay for the session anyway or at the very least send a generous gift card.

In short, act as if you really want to impress, and there's an extremely high chance she will do the same for you.

MAGGIE MCNEILL is a full-time sex worker and sex worker rights activist based in Seattle. Since 2010, she has written a daily blog, *The Honest Courtesan*.

How to (Legally) Make Your Own Off-the-Books Handgun

BUILD A GLOCK 17 USING PARTS FROM THE INTERNET

MARK MCDANIEL

photos by Todd Krainin

LET'S START WITH a disclaimer: If you have little to no experience with guns, it's probably not wise to try assembling your own. It can be dangerous to make a mistake—even deadly. There's no shame in buying a firearm from a reputable manufacturer and then taking a class to learn how to handle it safely, defensively, and intelligently.

But do-it-yourself has its appeal as well. For those who already have basic firearm know-how and competence with common tools, it's easy to make a gun that's just as safe as one bought from a store.

It's also perfectly legal in most American jurisdictions. That simple fact tends to be ignored by pundits and politicians in the debate over gun control. But if even moderately skilled people can create their own weapons at home—and increasingly they can—then passing laws to regulate commercial manufacture and sale starts to look awfully futile. While firearm restrictionists will likely soon be clamoring for laws to rein in private production, there's only so much they can do: Communicating instructions for how to build a gun is constitutionally protected speech, after all.

In celebration of the First Amendment, let's walk through how to make a weapon based on one of the most popular semiautomatic handguns in the world: the Glock 17, a full-size double-stack 9 mm pistol with a track record of reliability and

simplicity. Recently, third-party companies began marketing "frame kits" that allow private individuals to make guns that look and operate like Glocks and are compatible with Glock parts. There's a caveat, however: Their product includes excess plastic that, unless removed, prevents you from turning it into a functional weapon. By itself, the object they sell doesn't count as a firearm in the eyes of the law. Instead, it is colloquially known as an "80 percent frame" or an "80 percent receiver."

This will be the platform for our homemade gun.

HOW IS THIS LEGAL?

GUNS ARE REGULATED in various ways. The same is not true for an object that happens to be transformable into a gun by a skilled home hobbyist.

Despite the name, though, the difference between a gun and such an unregulated object isn't as clear-cut as some sort of "80 percent rule," says attorney Mark Barnes, a D.C. lawyer who specializes in issues involving the import, export, and manufacture of firearms. "The fact of the matter is that firearms design differs from gun to gun. As a consequence, the final judge on whether or not a physical object constitutes the frame or receiver of a firearm is the Firearms and Ammunition Technology Division of the Bureau of Alcohol, Tobacco, Firearms, and Explosives" (ATF).

If you send ATF an object, the bureau's experts will explain why it is or isn't a firearm according to two main laws. The Gun Control Act of 1968 defines a firearm as "any weapon…which will or is designed to or may readily be converted to expel a projectile by the action of an explosive," or "the frame or receiver of any such weapon." The National Firearms Act, meanwhile, says the frame/receiver is the "part of a firearm which provides housing for the hammer, bolt or breechblock and firing mechanism, and which is usually threaded at its forward portion to receive the barrel."

Eighty percent receivers are incapable, out of the box, of accepting a slide or trigger assembly. Turning one into a working gun takes some amount of drilling, filing, or millwork. As a result, ATF does not consider them to be firearms, and they can be bought outside the bureaucratic system that governs firearm sales.

Federal law demands that all commercial firearm purchases go through a registered Federal Firearms License (FFL) holder. Guns produced and sold by FFLs must be stamped with serial numbers, and the dealer must keep records of all sales.

Those restrictions apply to commercial transactions. But private individuals are allowed to make their own guns, Barnes explains, "as long as they aren't prohibited under federal, state, or local law from accessing, transporting, or receiving firearms." If you are not a licensed dealer, in other words, you can most likely purchase an 80 percent frame, remove the excess material, add a few parts, and turn it into a functional gun. No questions asked, no government paperwork, no background checks.

This is where the 80 percent Glock models shine. The frame kit and all other necessary parts can be legally ordered on the internet. Because the frame is made of polymer, hand tools will be enough to get the job done. You don't need an expensive computer numerical control mill or drill press—just a Dremel or similar automatic rotary device, a set of files, and some sandpaper.

After having their designs reviewed by ATF, companies such as Polymer80 and Lone Wolf released some of the first unfinished frames for the full-size Glock 17 and compact Glock 19. Typically, their designs include a few improvements over stock Glock frames, including a different grip angle, texture, and attachment system. For our build, we went with a Polymer80 PF940v2 purchased from Brownells.com. We also bought a complete Gen 3 Glock 17 slide and barrel assembly and a Glock lower parts kit (including trigger assembly) on eBay.

WHO MIGHT WANT TO DO THIS?

GUN SALES TYPICALLY soar when people have reason to fear that laws governing who can legally obtain different types of weapons are about to get more stringent. Following the Valentine's Day school shooting in South Florida, there was an uptick in anti-gun rhetoric. Firearm sales the following month broke the previous March record by a quarter-million.

And those are only the sales tracked through the FBI's National Criminal Background Check System. As worries over potential bans or even confiscations rise, some feel the urge to leave as small a paper trail as possible regarding their personal weapons.

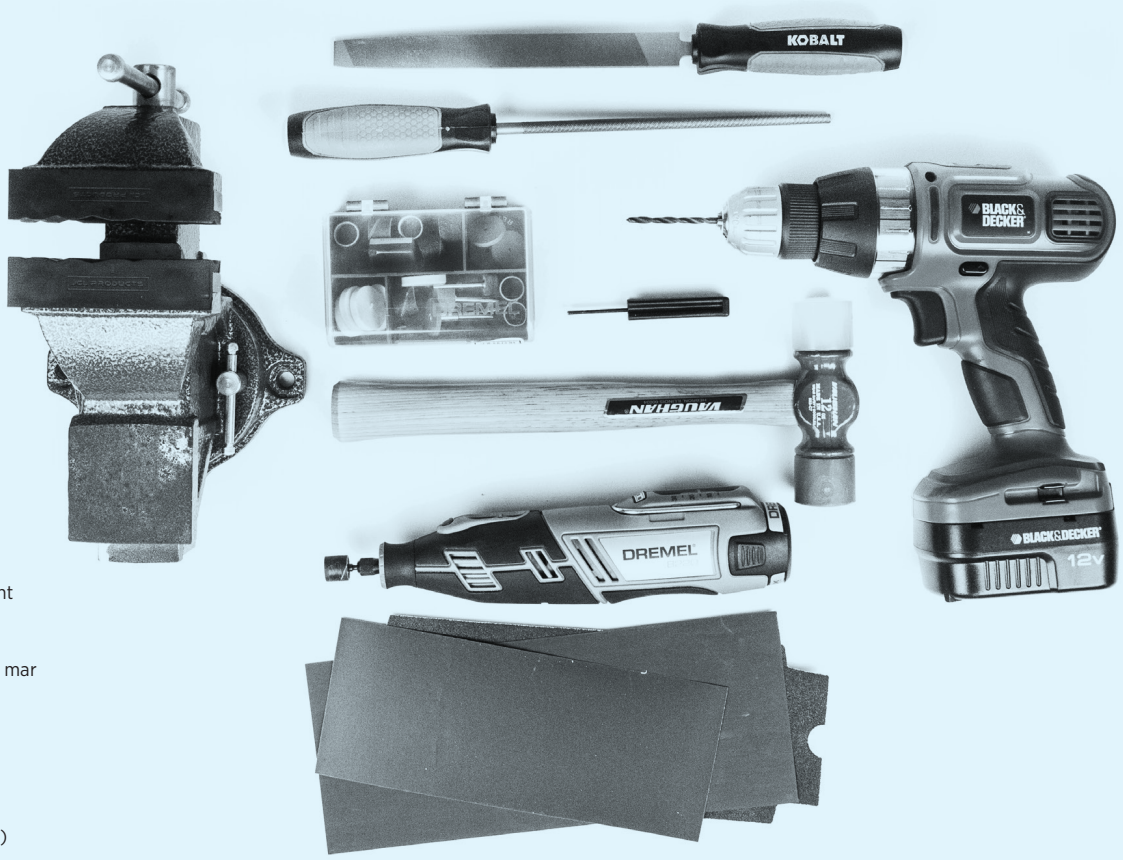
The easiest way to avoid government attention is to purchase your gun from a private seller. Most states minimally regulate such transactions, leaving Americans free to buy firearms from each other without much interference. But a secondary-market weapon is still marked with a serial number that can be traced back to the original owner, which means there is a path eventually leading to you.

If paper trails are your biggest worry, you may be thinking of grinding the serial number off a gun you purchase. This is a felony. Do not do this.

A better way to fly under the radar is to make the gun yourself. Firearms produced by individuals outside the FFL system don't require a serial number under federal law.

(Note that states may nonetheless require one. For example, California in 2017 mandated that all "ghost guns," or guns made by nontraditional manufacturers, be registered and have a serial number added to them. This will probably be hard to enforce. Still, you should be sure you know what laws are on the books in your state before going down this road.)

To remain anonymous, you'll need to buy the unfinished



TOOLS YOU WILL NEED:

- A Dremel or other rotary tool with a sanding drum
- A set of metal files
- Coarse and fine-grit sandpaper (we used 100-, 800-, and 1,200-grit)
- WD-40 and a firearm lubricant such as RemOil or Ballistol
- A hammer (preferably nylon, rather than metal, so as not to mar the frame)
- A flathead screwdriver
- A bench vise (optional but helpful)
- A power drill (optional; your rotary tool may be substituted)

frame and other parts with cash. It's doable, but it's likely to be a pain in the ass. Instead, most people shop online.

The internet has ushered in a golden age for small arms. It's easier than ever to learn about guns, purchase parts, and find places to train to use your weapon. If you want to know it or buy it, it's out there, thanks to the web. It's actually slightly more expensive to acquire the unfinished frame and parts to assemble a Glock yourself than it is to purchase one readymade, but everything you need is available at your fingertips.

The downside of credit cards and shipping addresses is that there will be a record in some form of what you buy. In the event of a ban (or if law enforcement has some reason to take an interest in you), the receipts can be subpoenaed.

Nothing is totally foolproof, but adding an extra layer of complexity to slow attempts by outsiders to locate your weapons might be worth it to you. For this experiment, we purchased all our parts on the internet. They were shipped directly to us, with no FFL middleman and no government registration.

Your home-crafted gun may not work as well as a factory Glock—though, with care and some modifications, it could work even better—but if you value privacy over price and don't mind a bit of tinkering, this could be a solution for you.

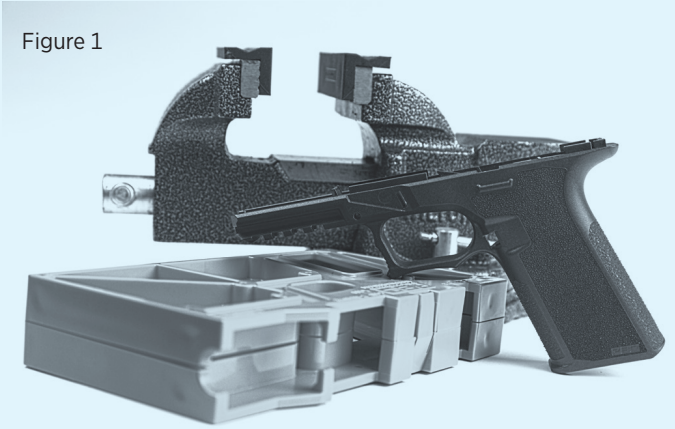
HOW TO FINISH THE FRAME AND ASSEMBLE THE GUN

TO FINISH YOUR gun from 80 percent, you'll need to remove the excess polymer that prevents the slide and trigger assembly from being attached. (The slide we used came already assembled, as did the trigger assembly.)

The frame is shipped with a jig—a device that holds the object you are working on and guides the tools you're using on it—that helps with sanding and drilling. Extending above the jig are the parts of the frame we'll be sanding off—we'll call them "tabs"—which are labeled on the jig with the word "REMOVE." Most unfinished polymer frames are finished in a similar manner. Consult the instructions if you choose another model.

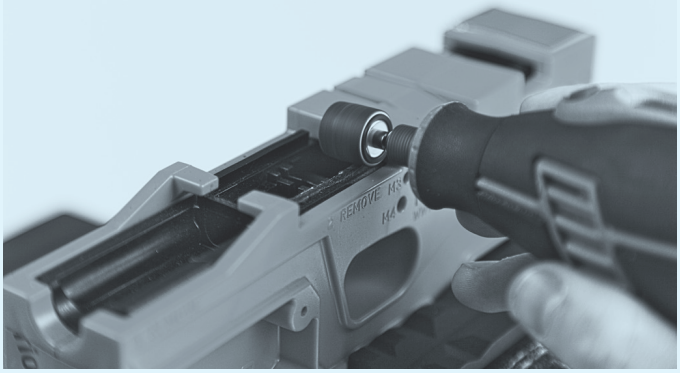
I am not, nor is anyone at *Reason*, a professional armorer or gunsmith—just an interested amateur who used the following techniques to make a usable weapon at home.

Figure 1



Assemble the needed supplies (Figure 1). Using a vise, secure the frame in the jig and make sure it is level. Optionally, tape the ends of the jig to ensure minimal movement of the frame.

Figure 2

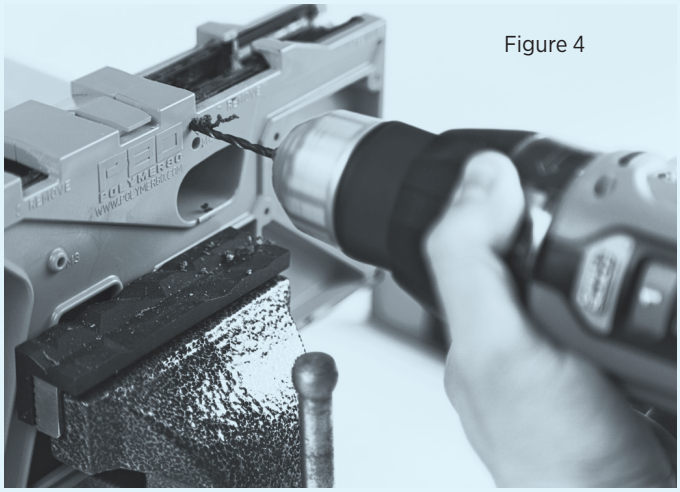


Using the Dremel and the sanding drum attachment, start to sand down the polymer tabs marked for removal (Figure 2). Be very careful. While you can use the Dremel for the entire process, it is much easier to make a mistake that way. Use the Dremel for most of the heavy lifting. In the next step, you'll continue the sanding by hand for a more precise and smooth result.

Figure 3

Once the majority of the material has been removed from all four tabs, use hand files to smooth the remaining material (Figure 3). Be sure not to go too far into the frame. The files should be used to remove the material in the corners that the sanding drum can't reach.

Figure 4



While the frame is still in the jig, drill the holes for the trigger assembly and rear slide rails (Figure 4). The exact placement and drill-bit sizes for these holes are marked on the jig. Use the supplied drill bits in either a hand drill or the Dremel for this step. It is important that you take your time, making sure to drill a perfectly straight hole.

When drilling, do not go through the entire frame from one side. Instead, alternate drilling on each side until you feel the drill bit break through the polymer. Use a sharp blade or a small file to clean up the holes on the inside of the frame.

Figure 5

Using the Dremel or a round file, remove the excess polymer from the guide rod channel (Figure 5). There's a *U*-shaped mark on the polymer indicating which section is to be removed. Like before, be cautious and take your time.

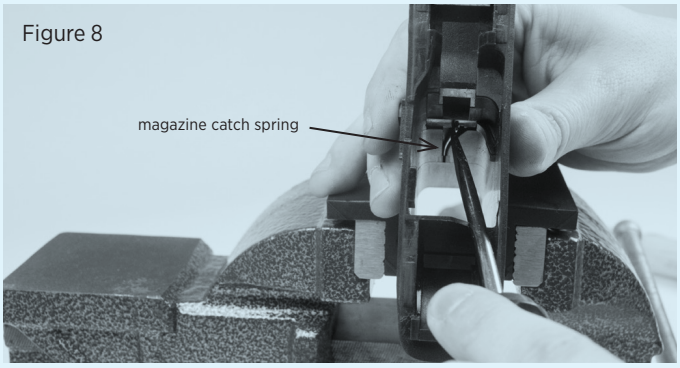
Figure 6

After drilling the holes for the trigger assembly, you can begin the final round of sanding (Figure 6). Start by spraying a small amount of WD-40 on coarse-grit sandpaper for a wet-sand effect. Going slowly to make sure you don't bite into the frame, sand off any polymer that remains where the tabs were, cleaning up the plastic burrs that may still be attached to the frame. Once the tabs are totally flush with the rest of the frame, use the fine-grit sandpaper with WD-40 for a polished effect.

Figure 7

Now you're ready to start assembling the frame. Install the slide lock by inserting the slide lock spring into the top of the frame. Using a flathead screwdriver, depress the spring and push the slide lock into the channel on the side of the frame above the spring (Figure 7). The small lip on the slide lock should face toward the rear of the frame.

Figure 8



To install the magazine catch, insert the magazine catch spring through the top of the frame and into the channel at the font of the magwell (i.e., the hollow space inside the grip that will accept the magazine). Push the magazine catch in through the side of the frame. With your flathead screwdriver, pull the top of the magazine catch spring away from the frame, allowing the magazine catch to slide underneath. Use the screwdriver to guide the magazine catch spring into the slot on the magazine release (Figure 8).

Figure 9

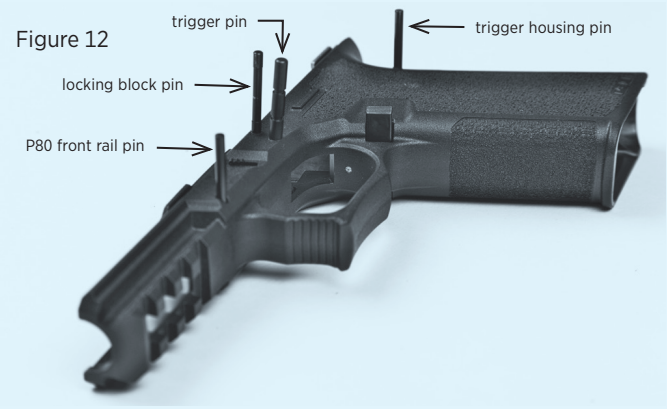
Figure 10

Insert the front and rear slide rails into the frame (Figure 9). Using a hammer, tap them into place (Figure 10).

Figure 11

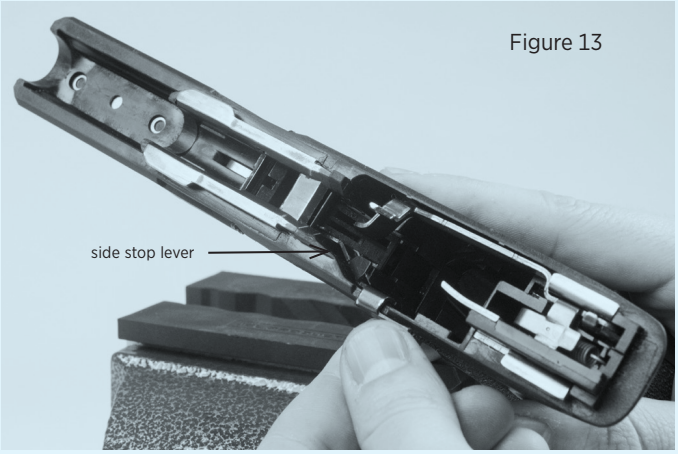
Insert the trigger assembly into the rear of the frame (Figure 11).

Figure 12



Using a hammer, drive in the trigger housing pin, the P80 front rail pin, and the locking block pin (Figure 12).

Figure 13



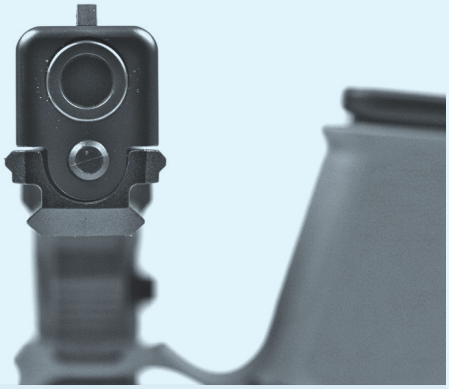
Insert the slide stop lever. The *U*-shaped spring should rest underneath the locking block pin, and the hole should line up with the trigger pin hole (Figure 13). Drive in the trigger pin.

Figure 14

Figure 15

The frame is ready to accept a slide assembly (Figure 14). Lubricate the rails and attach the slide to them (Figure 15). They may need some additional polishing or filing to allow the slide to move freely.

Inspect the frame and slide, ensuring everything functions properly before firing, as you would with any new firearm.

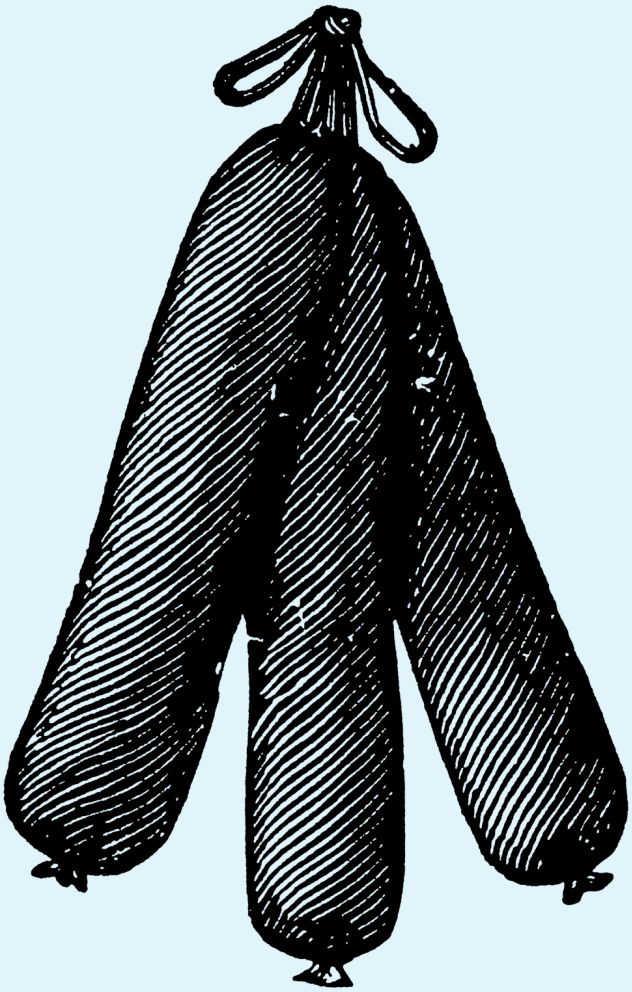


Congrats! You're now the owner of an off-the-books handgun.

MARK MCDANIEL is a producer at *Reason*. For a video version of this tutorial, visit reason.com.

Don't Let Uncle Sam Seize Your Salami

ALEC WARD



YOU'RE ON A plane, returning home from a romantic tour of the Italian countryside. The cabin lights flicker on and you're confronted by flight attendants passing out slips of official-looking blue cardstock: customs forms.

After scrounging a pen out of the bottom of your carry-on, you start to fill out the cramped response fields. Name, address, flight information. Back to the carry-on again, because who on Earth knows his own passport number? Finally, you come to the declaration section, and begin to tick off negative responses to the bizarre interrogatories. Bringing back soil? No. Seeds? No. Disease agents, cell cultures, or snails? No. Food or meat?

Your stomach drops as you remember the rustic charcuterie you purchased at a quaint butcher shop in Naples. Delicious, and not cheap, either. What to do? The once-boring form suddenly seems daunting. You're no scofflaw, but what will happen if you check "yes"? You don't want Uncle Sam to seize your salami. (That already happened once on this trip. Thanks, TSA.)

Subduing your law-abiding conscience, you cross your fingers, apologize to your divinity, and mark the box beside "no." OK, now what?

Probabilistically speaking, the answer is "likely nothing." Customs and Border Protection (CBP) doesn't usually conduct thorough searches of incoming commercial airline passenger baggage. Consequently, there's a decent chance your smuggled sausages slide through undiscovered.

But from a legal perspective, things look dicier. If you present your falsified form to a customs officer, you're technically in violation of a whole host of laws. And how costly is getting caught? Turns out it's hard to know. The applicable regulations are complex, numerous, redundant—and vague.

Say your goods are detected by one of CBP's trained food-sniffing dogs (yes, apparently the government believes dogs have to be trained to sniff out food). Depending on the stage of the inspection process, whether or not you've already handed over your form, what exactly the dog handler asks you, and what exactly you say, you could be guilty of import violations or criminal smuggling.

Civil import violations carry penalties tied to either the value of the article itself or to the taxes you would have been assessed if you'd declared it. In practice, criminal smuggling seems to be reserved for incidents involving drugs, but there's nothing in the law as written to prevent a prosecution for illicit meat.

At a minimum, you're likely guilty of "failure to declare," a catchall offense that seems to be popular among CBP officers who work in airports. Unlike the more technical importation violations, which apply only to taxable goods (a category for which your charcuterie is unlikely to qualify), you can be guilty of "failure to declare" even if the thing you're trying to bring in isn't subject to a tax, duty, or other restriction. Mere failure to disclose its presence is enough to create liability.

But depending what exactly your meat is made of, where it comes from, and whether any export-import treaties are applicable in its case, you may be breaking the law just by carrying it into the country. The relevant statute says the penalty for failing to declare a "controlled substance"—which in this case means anything that can't be legally imported, not just narcotics—is $500 or 10 times the value of the item, whichever is higher. If the item is not a controlled substance, you're still supposed to be assessed a fine equal to its value, plus any applicable taxes, plus a portion thereof again as yet another penalty.

nicoolay/iStock

But anecdotal evidence suggests that because of confusion around the rules, customs officers have a tremendous amount of discretion regarding how to handle violations. Anthony Bucci, a spokesman for CBP's New York field office, says that in the context of agriculture enforcement, whether a fine is imposed (and how steep it is) often comes down to whether an inspecting officer thinks the passenger has deliberately tried to pull a fast one on him.

"It's not a guarantee that the [failure to declare] fine will be assessed—it could be just a warning," he says. "The fine is more in the cases where the person is being dishonest, is not being truthful."

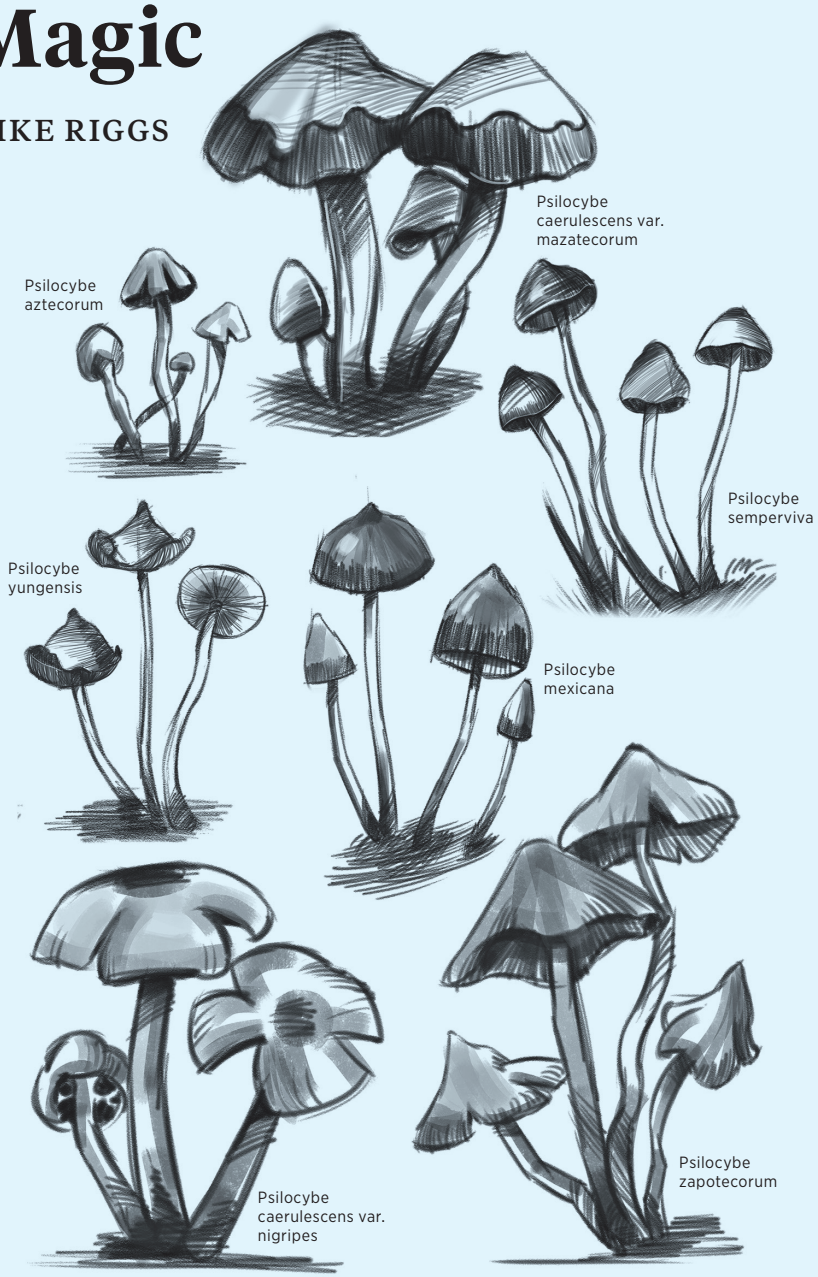
Online accounts from folks who report having been discovered transporting undeclared victuals variously report assessment of the full $500 levy, a lesser $300 levy, or no levy at all. A clip from a National Geographic television show about customs enforcement in New York City shows an airline passenger being fined $300 for a sandwich discovered in a carry-on bag he says his mother packed for him. On the eye-popping end of the spectrum, Columba Bush, wife of former Florida Gov. Jeb Bush, was reportedly fined $4,100 for failing to declare $19,000 in clothing and jewelry she bought on a trip to Paris in 1999.

If you are charged a penalty, good luck contesting it. On-the-spot fines imposed at the airport are generally not adjudicable, according to Bucci. "We have a cashier's window right inside our federal inspection site," he says. "If you have to pay a fine, you have to pay it right there....The burden of admissibility into the United States is on the traveler. That traveler has to, for lack of a better word, prove their admissibility 100 percent." ⓡ

ALEC WARD was the Spring 2018 Burton C. Gray Memorial Intern.

Mushrooms Aren't Magic

MIKE RIGGS



WHEN SPANISH CATHOLICS subjugated the Mesoamericans, they eradicated a religion but not its chief sacrament. Psilocybin mushrooms continued to grow throughout Central America and to clandestinely fuel the trips of indigenous psychonauts. In the 1950s, the Mazatec shaman María Sabina led an American banker named Gordon Wasson and his wife in a mushroom ceremony, and the couple returned to the U.S. as proselytizers. Today, psilocybin mushrooms are more popular and easier to cultivate than at any point in recent memory, thanks to the internet's ability to disperse knowledge in much the same way that *Psilocybe mexicana* spreads its spores.

But it wasn't always so. The first widely available American treatise on home growing was 1976's *Psilocybin: Magic Mushroom Grower's Guide*. Authors Ter-

ence and Dennis McKenna published under the pseudonyms O.T. Oss and O.N. Oeric, though in a fun twist, Terence wrote the forward under his real name. In addition to trippy illustrations juxtaposed with chemical diagrams and laboratory photos, the brothers provided detailed instructions for achieving the four major stages of growth: extracting spores (the fungal equivalent of seeds), cultivating a batch of mycelium (the vegetative part of a fungus), inoculating a sterile medium with the mycelium, and then simulating the conditions of a humid forest floor in order to produce mushrooms.

Forty years later, the book is useful mostly as a window into Terence McKenna's imagination. "I am old, older than thought in your species," he envisions a mushroom saying to a human. "By means impossible to explain because of certain misconceptions in your model of reality all my mycelial networks in the galaxy are in hyperlight communication across space and time." The actual growing advice, however, is archaically complex (see: using agar, a growing medium common in labs but unnecessarily complicated for home mycologists).

Several decades of experimentation and knowledge sharing have led to a much simpler orthodoxy, with most amateur mycologists now of one opinion about the best materials and methods. For beginners, an internet search for "PF Tek" will return a nearly foolproof method for growing small amounts of *Psilocybe cubensis* at home. (It will also point you to forums where every question you can possibly imagine has been answered in great detail.) All the materials can be purchased at your local hardware and health food stores, save one: the actual spores.

Psilocybin spores are legal to possess for microscopy purposes in all but three states (Georgia, Idaho, and California do not allow their possession for any reason). They can be ordered, along with microscope slides, from vendors such as Spore Works. But the minute you attempt to cultivate them, you will be breaking the law.

Here I should note that the instructions are nearly, but not entirely, foolproof. Growing any type of mushroom—culinary, medicinal, or magic—is a challenge for even the greenest thumb. Paul Stamets, America's premier populizer of citizen mycology, writes in his 2005 book *Mycelium Running* that success at growing mushrooms relies on a number of factors, "some obvious and some mysterious." Nobody talks this way about growing cilantro in a kitchen window sill.

That's because plants need only sunlight, water, soil, and to not be forgotten about entirely, while mushrooms require parenting. Most plants are no worse for wear if you accidentally ash a cigarette on their heads or leave town for a long weekend and don't water them. You will find them sickly and resentful-looking when you get back, but wet their roots and they'll forgive you. Not mushrooms. A single misstep early on will kill your experiment dead in its tracks. One day, your babies will be reaching their delicate hyphae through a seemingly sterile substrate; the next they'll be hampered by green patches of *Trichoderma* and cottony tufts of cobweb mold.

In fact, your mushrooms may falter even if you do everything right, which probably seems like a paradox: How can it be so hard to grow them in the relatively sterile confines of a temperature-controlled home, yet so easy to find them bursting out of piles of cow shit?

It helps to think of mushroom cultivation as microscopic world building rather than plant growing. If you prepare a clay pot for a seedling and place it on a window sill inside your home but never actually plant anything, you can reasonably expect the pot to remain barren indefinitely. When you make a good home for mycelium, however, you've made a damp, welcoming environment for all manner of tiny, invisible, and invasive travelers. Do nothing with that container, and unwelcome life will eventually find a way there, just as it does on a forgotten piece of sharp cheddar in the back of your fridge.

One must make peace with failure—initially but also throughout one's mycological journey. There's only so much you can do to aid *Psilocybe cubensis* in its efforts to reproduce (for that is all mushrooms are to mycelium: a vehicle for spreading spores). Competing species of fungus and bacteria also want to pass along their genetic material and will fight valiantly to do so. Practicing good hygiene, following instructions, and taking notes will give your preferred species a leg up, but ultimately you can only watch and hope that the genes you're cheering are both selfish and strong.

Even the most meticulous mycologist will fail at some point, probably repeatedly. But every embryological stage you get to witness, even if it does not culminate in fruiting, will fill you with wonder. That first vein of mycelium, creeping along the glass wall of a Ball jar, will be to you as veins of gold were for western prospectors. Watching it search out other patches of mycelium to form a network will have you marveling at the miracle of life. The rich, sweet, earthy smell of the budding fungus—be it *Psilocybe cyanescens* or *Pleurotus ostreatus*, a delicious oyster mushroom—will be more fragrant to you than the finest myrrh. Should you bear witness to primordium protruding from a mycelial mat, you will want to shout from the rooftops. And if you are so lucky as to taste the literal fruit of your efforts, you will be forever different because of it.

Your friends will think you're weird. But you will know something they don't about how life happens on this wonderful planet. And if you approach your experience with the right mindset and in the right setting, you will learn why the Mesoamericans called psilocybin the "food of the gods." ●

MIKE RIGGS is a reporter at *Reason*.

Megalaxmadi/Fiverr

This Is Not a Pot Pipe

JACOB SULLUM

IF YOU TAKE an apple from your fruit bowl, you have committed no crime. If you take a knife and carve a right-angled channel through the apple, starting at the top and ending on the side, you are still in the clear.

But the moment you think about covering the top hole with perforated aluminum foil to hold a nugget of marijuana that you will light while sucking on the side hole, you have transformed that innocent apple into contraband. Possessing it could earn you penalties ranging from a fine (up to $500 in Texas, where I live) to a jail sentence (as long as a year in Pennsylvania, where I grew up).

In both Texas and Pennsylvania, drug paraphernalia is defined by intent. A hookah is legal as long as you plan to smoke tobacco in it, while a briar pipe is illegal if you plan to smoke marijuana in it.

For manufacturers and distributors of drug paraphernalia, criminal liability under state law generally depends on knowledge: Did the seller know (or should he have known) his merchandise would be used to consume illegal drugs? Those "for tobacco use only" signs in head shops are meant to maintain a pose of ignorance.

That pose will not help merchants much under federal law, which according to the Supreme Court relies on an "objective" definition of paraphernalia, based on "a product's likely use," as opposed to a "subjective" definition, based on "the defendant's state of mind." Online sellers of equipment that could conceivably be used to consume cannabis nevertheless prefer caginess to candor.

VaporNation, based in Torrance, California, describes its main product line as "personal devices that heat materials at temperatures just below the point of combustion, extracting the flavors, aromas, and effects of herbs and waxes with much less smoke." The company, which in addition to vaporizers carries grinders, containers, glassware, and water pipes, does not specify what sort of "herbs and waxes" it has in mind, which is probably for the best. Although marijuana accessories, like marijuana itself, are legal in California, they remain illegal in most states, and selling them is still a federal felony punishable by up to three years in prison.

Since state-licensed businesses selling actual marijuana so far have gone mostly unmolested by federal prosecutors, the chances of legal trouble for VaporNation may seem small. Then again, the company ships its products to customers throughout the country, which is not the sort of thing a marijuana merchant who wanted to avoid federal attention would do.

If VaporNation ever attracted such attention, the vague description of its products' intended use probably would not save it. But a little-noticed clause in the federal paraphernalia statute might. The law says "this section shall not apply to…any person authorized by local, State, or Federal law to manufacture, possess, or distribute such items."

Steve Fox, a lawyer who directs the National Cannabis Industry Association's Policy Council, thinks that language should cover businesses that sell marijuana accessories in compliance with state law. U.S. Customs and Border Protection (CBP), which last year seized a shipment of lockable storage cases ordered by Stashlogix, a Boulder, Colorado, company that sells "thoughtful, secure and discreet stash bags" for "medicine, tobacco & other stuff," seems to disagree.

In a letter to Stashlogix, CBP explained that the cases would have been perfectly legal without the carbon pouches that accompanied them. As far as the agency was concerned, those odor-absorbing inserts gave off the unmistakable smell of illegality. ⓡ

JACOB SULLUM is a senior editor at *Reason*.

Joanna Andreasson