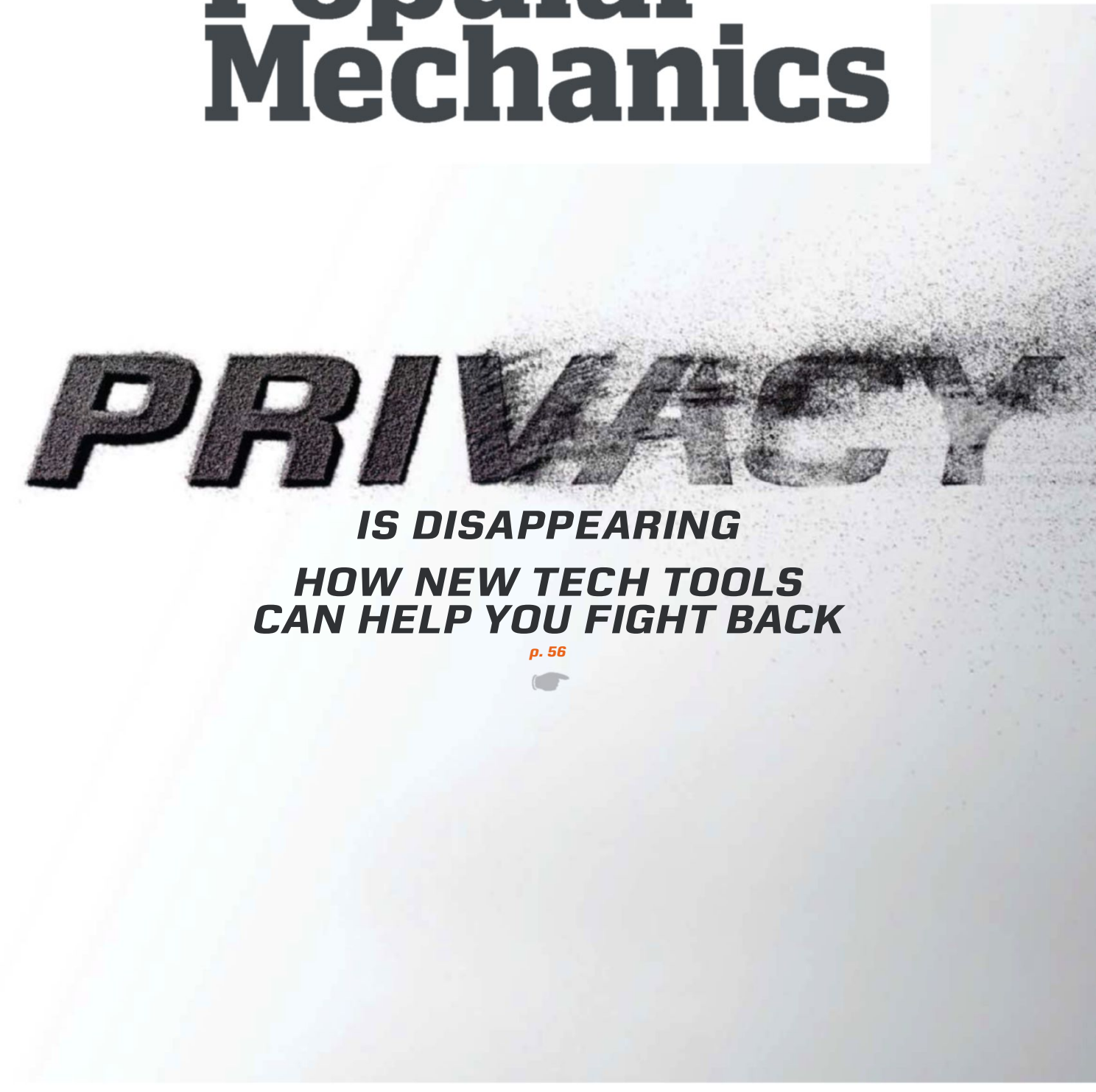
TOP TECH TRENDS FOR 2014 p. 52 HUMAN-POWERED FLIGHT p. 72

Popular Mechanics



IS DISAPPEARING

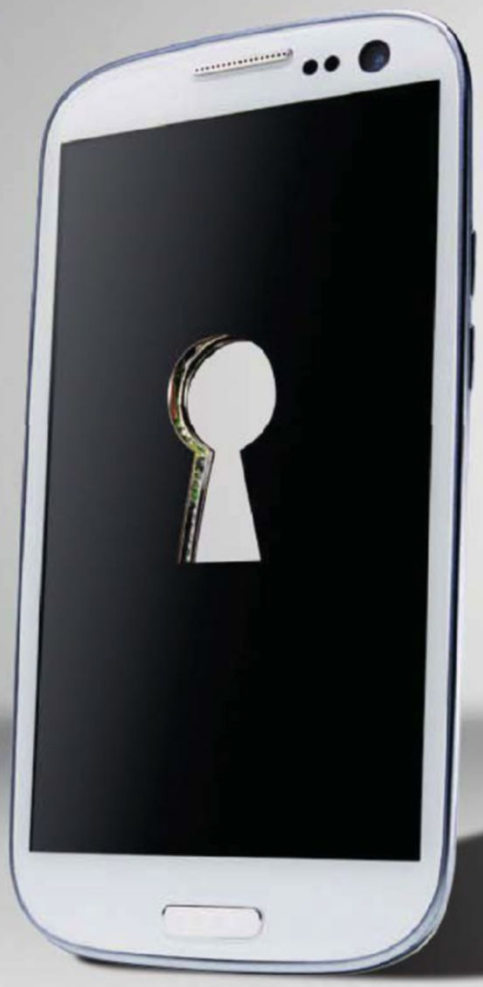
HOW NEW TECH TOOLS CAN HELP YOU FIGHT BACK

p. 56

TECH HOME AUTO ADVENTURE SCIENCE

ISSUE FEBRUARY 2014
Since 1902

THE DIGITAL SPIES ARE WATCHING YOU—MARKETERS, THE NSA, IDENTITY THIEVES, ALL KINDS OF SNOOPS. BUT THE BATTLE'S NOT OVER. HERE ARE SEVEN BIG CATEGORIES OF PERSONAL TECH, AND HOW YOU CAN SECURE THEM.



IT'S TIME TO FIGHT FOR YOUR

PRI

PRIVACY, WE SAY, is about to come roaring back. No, it's not too late. Yes, we know that Google monetizes both our emails and our search histories. It's true that data brokers market our personal dossiers, listing everything from our favorite blogs to our old parking tickets (identity thieves must love it). And NSA leaker Edward Snowden really did prove the paranoids right: The United States government spies on everyone. Now, we agree that security agencies have a vital responsibility to track terrorists, but that mission can't require all citizens to live in a surveillance state. Feel you have nothing to hide? That assumes the data will always be used to defeat terrorists, not to monitor activists, let alone to stalk ex-girlfriends—yes, NSA employees have done that. Here's the other side to the privacy-is-dead argument. You can fight the privacy erosion that technology has enabled using tools that technology provides. And when you protect your data—using encryption and other tools—you incidentally bolster the argument that security is the norm. At least it should be. Privacy is not dead but simply suffering from neglect. It's your job to revive it.

BY **DAVEY ALBA**

PHOTOGRAPH BY **TERU ONISHI**
PROP STYLING BY SARAH GUIDO

TECH: WEB BROWSERS

TO DO: DEFEAT TRACKING SOFTWARE

Web browsers work in two directions: You use them to learn about the world, and snoops use them to learn about you. The sheer number of identifying files, or cookies, downloaded onto our computers can surprise even jaded digital natives. Many cookies are helpful—keeping you logged in to a service, for instance—but others exist purely to help marketers target their sales pitches. An online tool maintained by the Network Advertising Initiative can reveal who is collecting information on you; a browser we tested was being tracked by 82 firms, with

•

TYPOGRAPHY BY SINELAB

names such as AppNexus, Criteo, and Datalogix.

Cookies can be cleared, but new methods for tracking online use will be harder to circumvent. For instance, some companies use browser fingerprinting, which looks for distinctive patterns of computer settings, such as installed fonts and time-zone details, to home in on a user's identity. Google and Microsoft are also working on a new form of cookie-less identification: unique IDs with tracking that reaches beyond the desktop and into the user's browsing activities on smartphones and tablets. Google's system potentially could be used to tie together data across all its products—Gmail, the Chrome browser, and Android phones. In addition to tech firms, the U.S. government can monitor your digital trail through your browser. Among last year's revelations: The NSA has tapped into the fiber-optic cables that make up the Internet's backbone, and, through the Marina metadata application, the agency can track an individual's browsing history, social connections, and, in some cases, physical locations.

Routine fix: To practice good browser hygiene, regularly clear your cookies and your browser cache. There are a number of browser add-ons that can shrink the deluge as it pours in. For instance, AdBlock Edge blocks ads and third-party trackers. The Disconnect add-on lets you see and prevent otherwise invisible tracking of your browsing history. (Both add-ons work with Firefox and Chrome; Firefox is preferable because it's an open-source browser.) **Extreme fix:** Organizing resistance to a totalitarian state and need real anonymity? Download the Tor Browser Bundle. Tor has become famous as a secure way for activists, journalists, and, yes, some criminals to browse the Web. Tor bundles your data into encrypted packets and directs it through a worldwide volunteer network of more than 3000 servers, hiding your location and making your data more difficult to read along the way.

There are two downsides to Tor: First, it's slow, because your data is sent through at least three relays, with each relay donating different amounts of bandwidth to Tor users. Second, merely downloading it can draw government scrutiny. The NSA has reportedly developed a system called FoxAcid to insert eavesdropping applications into the machines of Tor users. However, the agency admitted in a leaked Snowden document, "We will never be able to de-anonymize all Tor users all the time." A virtual private network (VPN) adds a different kind of protection by encrypting all outbound computer communications. Combine Tor with a VPN and you've got even tighter security.

TECH: SOCIAL NETWORKS

TO DO: RAMP UP PRIVACY SETTINGS

In 2011 an Austrian law student named Max Schrems asked Facebook to provide all the data it had collected on him, taking advantage of an obscure provision in a European data-protection law passed in 1995. Schrems initially received only a fraction of his data. He protested, and eventually a CD showed up at his door that held a 1222-page PDF, which included employment information, relationship statuses, pokes, old chat conversations, and geotagged photos—most of it information that Schrems thought he had deleted. Such data is being monetized by tech companies in increasingly invasive ways. Google's Shared Endorsements feature, for instance, allows the company to

E-ZPass tags capture a car's location data at toll plazas. The information can be used in civil court cases, such as divorces. Tag readers can also be used to monitor traffic flow along any road.

PHOTOGRAPH BY ASSOCIATED PRESS

ILLUSTRATIONS BY **AMANDA LANZONE**

PRIVACY MAKEOVER

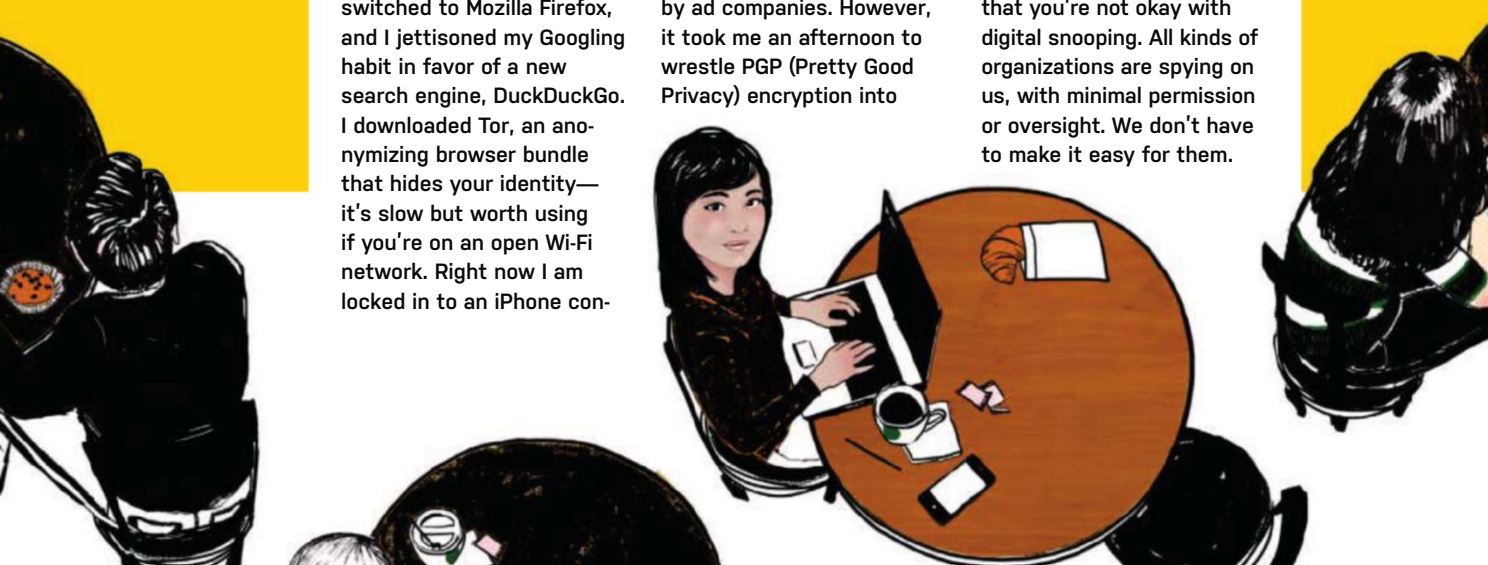
HOW POPMECH TECH EDITOR DAVEY ALBA TRIED FOR TOTAL DIGITAL SECURITY.

PROUD TECHNOPHILE—that's how I'd describe myself. I've built a 3D printer from mail-order parts. I once tracked down an iPhone thief using sneaky digital tools. My smartphone, at last count, has 303 apps. But testing seemingly every digital product released has a downside: It means I have bigger privacy vulnerabilities than most people. And for all the attention I pay to technology, I've never worked particularly hard at protecting my data—I always used default privacy settings and the same, sloppy online tools most people choose. No longer. After interviewing dozens of computer science researchers, cryptographers, and security professionals and learning how easily digital snoops can access personal data, I decided to change my ways. Every expert's top suggestion: Use open-source software, because the NSA works with tech companies to weaken encryption in proprietary software. "It's much harder to build in back doors in open-source," Matthew Green, a computer security expert at Johns Hopkins University, told me. "The eyeballs are on it." I switched to Mozilla Firefox, and I jettisoned my Googling habit in favor of a new search engine, DuckDuckGo. I downloaded Tor, an anonymizing browser bundle that hides your identity—it's slow but worth using if you're on an open Wi-Fi network. Right now I am locked in to an iPhone contract, but next time I'll go with Android, which is open-source. So far, so easy.

Next, I set about installing encryption software on my laptop and phone. Honestly, I'd never even heard of some of the tools my sources recommended—with names like Cryptocat, Autistici/Inventati, and GNU Privacy Guard. Downloading a secure instant-messaging client was a cinch. So was adding plug-ins to my browser to block tracking by ad companies. However, it took me an afternoon to wrestle PGP (Pretty Good Privacy) encryption into my email, partly because I insisted on learning how to encrypt my Facebook messages too. I started using a password manager, then promptly forgot the long master password I'd created. But I worked through the mishaps and felt much more secure once I was done.

But there was a rub: Privacy is a lonely world. I had an encrypted phone service and text messaging—and no one to talk to. The first time I fired up my secure texting app, Silent Text, I had exactly one contact on my list: Bruce Schneier, the cryptographer who'd recommended it. But rather than give up, I started cajoling my friends into enabling encryption on their own systems so that we could communicate. (I probably have lots of invisible new friends too. The NSA reportedly flags people who download encryption software—I imagine I'm now on the agency's radar.)

Is increased security worth the trouble? I say yes. Realistically, it may be hard to adopt some of these tools, the ones that require your friends to sign up as well. But if there's ever been a time to advocate for privacy technology, this is it. Downloading encryption tools sends a clear message that you're not okay with digital snooping. All kinds of organizations are spying on us, with minimal permission or oversight. We don't have to make it easy for them.



DIGITAL SAFETY ZONES

Where do you land along the privacy spectrum? Side with the easy-going online libertines and you'll never have to remember another password—but everyone from spambots to NSA spooks will have their way with you. Join the Luddite camp, avoiding all digital entanglements, and you'll be safer but isolated. Most of us will be happiest somewhere in the middle. Choose wisely, digital dweller.

The Man With No Secrets —at All

Security level: 1

Profile: You're a digital exhibitionist—and an identity thief's perfect target.
Digital tech: One password to rule them all (last four of your Social Security number should do it); unsecured Wi-Fi; phone Password Lock set to Off.
Social networks: Facebook, Snapchat, Pinterest, Twitter, Instagram—you name it. Privacy settings? What are those?
Commerce: The more retail loyalty programs you can join, the better you like it.

include a Google Plus user's name and photo alongside ads being shown to his social contacts, if the original user had indicated some interest in the product. And potentially such data could also be pored over by recruiters, cybercriminals, and stalkers.

Routine fix: Use strong privacy settings on each of your social networks, placing limits on who can see your posts. To block tracking software associated with the Share buttons on many websites, install Disconnect, an extension that disables such widgets. Also, log out of social networks when you're finished, and routinely clear cookies. **Extreme fix:** Opt out of social media—invite your friends to a barbecue.

TECH: AUTOMOBILES

TO DO: GET USED TO IT

In early 2012 a tinkerer with the Internet alias Puking Monkey hacked a plastic "moo cow" toy to sound an alarm every time his E-ZPass was read. This RFID-enabled device is used to pay bridge and highway tolls throughout much of the East. But during a test drive in July 2013 the cow lit up and wailed in Manhattan, even when the car was nowhere near a toll plaza. The unseen E-ZPass readers had been installed to help monitor traffic flow—but that didn't pacify the hacker. "If nontoll tracking is benign," asks Puking Monkey in an email, "why is it not disclosed when you sign up for an E-ZPass?"

There are ways to avoid that kind of tracking. But you can't do too much about the really big guns of automotive surveillance: the tens of thousands of automatic license-plate scanners deployed across the country. In Grapevine, Texas, to give one example, 14,547 vehicles were photographed in one day, and up to 2 million plates are currently stored in a database. Most law enforcement agencies can still set their own policies on the use and retention of the data (it varies by state); many

ILLUSTRATIONS BY AMANDA LANZONE

You Floss Nightly—and Clear Your Web Cache

Security level: 2

Profile: Sure, you know the NSA and Target are both listening in. Creepy? Sort of. You'll take precautions—but you're not giving up Scramble With Friends just to make a point.
Digital tech: For Web browsing, privacy add-ons (e.g., HTTPS Everywhere, Disconnect); for email, two-step verification and strong passwords; WPA-encrypted Wi-Fi.
Social networks: All networks, but with strong privacy settings and a password manager.
Commerce: Amazon Prime, baby . . . You can't give up everything.

Paranoid? No, Realistic

Security level: 3

Profile: They laughed at your talk of government surveillance, but that was before Edward Snowden. Who's paranoid now?
Digital tech: VPN (virtual private network), OTR (Off The Record) instant messaging for laptops, and Silent Circle for mobile phone calls; PGP (Pretty Good Privacy) email encryption.
Social networks: Offline only—you meet your buddies at the Def Con Hacking Conference.
Commerce: No loyalty cards; you give "Jenny's Number" (XXX-867-5309) to store clerks to look up "your" account.

Welcome To the Encrypted Zone

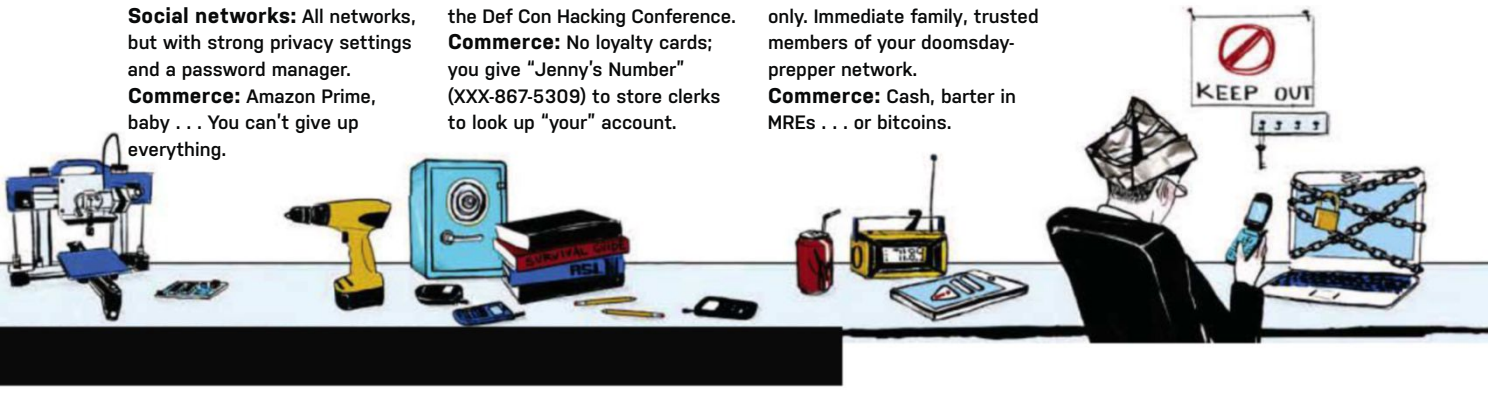
Security level: 4

Profile: You're a CIA agent or democracy activist in a totalitarian state. Or maybe you just think like one. Welcome to the privacy rabbit hole.
Digital tech: Air-gapped computers (meaning no Web connection) for sensitive files; burner phones; the Tor bundle with VPN. Open-source technology.
Social networks: Offline only. Immediate family, trusted members of your doomsday-prepper network.
Commerce: Cash, barter in MREs . . . or bitcoins.

Living Off the Grid, Under A Rock

Security level: 5

Profile: You don't want to worry about digital snooping—ever. So you've gone offline.
Digital tech: Does finger painting count? Absolutely no computers.
Social network: Other woodland creatures, your reclusive aunt.
Commerce: Cash, foraging for edible roots.



have no policy at all. In addition to all this, cars are themselves data-sharing devices—electric cars can upload data to their manufacturers, and connected services such as GM's OnStar and the Ford SYNC infotainment system send information to the cloud. But the most widespread in-car device is the event data recorder (EDR), which tracks seatbelt use, speed, steering, and braking, among other bits of vehicle data. This data comes into play during accident investigations. Ninety-six percent of cars built in 2013 have the devices; they will be required in all new cars starting next September.

Routine fix: You can store RFID devices such as an E-ZPass in a read-prevention holder until you get to a tollbooth. Or simply pay cash—though that option is going away on some roadways. There's a lot of chatter about techniques to defeat license-plate cameras, but it's unclear whether these are legal or even effective. **Extreme fix:** When it comes to black boxes in cars, the best approach is to know your legal rights—or, better yet, just to drive safely. Really hate being watched? Buy an old car that predates black boxes.

TECH: INSTANT MESSAGING

TO DO: CLEAR OLD CHATS

Instant messages seem fleeting, but they're not. The messages are stored, at least briefly, on the IM service provider's servers, and, unless you delete them, on your machine and your partner's. And unencrypted messages are vulnerable to interception as they travel from your device through your ISP's network to your IM service provider (Google, AOL, Yahoo, Microsoft, or whomever) and then out to your friend's computer. But does anyone actually snoop on IM conversations? Well, the U.S. government does, for one. Snowden leaks reported in July 2013 revealed the existence of XKeyscore, an NSA program run in cooperation with security

agencies in New Zealand and Australia that, among other things, lets agents surveil IM correspondence, often in real time.
Routine fix: Delete your chat records, in case anyone gets hold of your phone or laptop. You can stop recording future chats by changing the settings in your IM client. **Extreme fix:** The gold standard in IM encryption is OTR, or Off The Record (not to be confused with Google's proprietary Off The Record chat feature, which isn't secure). OTR uses "perfect forward secrecy," which means a fresh set of encryption keys is created every time one partner in the chat sends a new batch of messages. Note: Even participants in the chat won't be able to review old messages. As Ian Goldberg and Nikita Borisov, the designers of the OTR protocol, explained in an email, "The only record of the conversation is your memories."

TECH: EMAIL

TO DO: TURN ON OPTIONAL SECURITY TOOLS

ADI KAMDAR, ELECTRONIC FRONTIER FOUNDATION

The content of your emails can be less revealing than the metadata—the record of which contacts you correspond with and how often. Through a program called Stellar Wind, the NSA logged metadata on email communications for 10 years, and from 2007 to 2011 the data included bulk information on Americans. In a separate effort, the government agency has been scooping up hundreds of millions of contact lists from around the world, at a rate of 250 million people a year.

"TOO OFTEN THE DISCUSSION ABOUT PRIVACY DIGRESSES FROM THE ISSUE OF CONTROL. PEOPLE DESERVE THE POWER TO KNOW WHAT'S GOING ON, AND TO SAY NO OR SET LIMITS ON WHO CAN USE THEIR DATA. MAKING SURE GOOD CHECKS ARE IN PLACE IS SOMETHING THAT WE, AS BOTH CITIZENS AND CONSUMERS, CAN AND SHOULD FIGHT FOR."

One piece of fallout from that spying has been the shuttering of two services that until recently offered a high level of protection—not just against the United States government but also against repressive regimes and criminal organizations. Ladar Levison, the owner of Lavabit, a Texas-based secure email service, closed down operations in August after he was asked to hand over the encryption keys that protected his site to the FBI, which would have given the government access to all user data. The FBI said it was just interested in Lavabit's most famous user, Edward Snowden—but refused Levison's offer to provide access to that account only. A few hours later the encrypted communications company Silent Circle announced that it, too, was closing its email operations because, while the messages sent through its service were encrypted, email protocols—SMTP, POP3, and IMAP—leave user metadata open to spying. "We decided that our email service was too much of a risk for us and our customers," Silent Circle's Jon Callas says. "While it might have been a good idea six months before, it wasn't a good idea in a post-Snowden world." The companies have since teamed up to develop a new service, called Dark Mail, meant to secure both the content of an email and its metadata—the encryption will only work among Dark Mail users.
Routine fix: Ordinary email protocols make it impossible to hide metadata information, but there are ways to secure the content of your messages. Check that you're using the common Internet security protocols, SSL and TLS, when you're on webmail. (The browser's address line will start with https, and a small padlock appears.) If you're using a desktop mail client, make sure you're connected via SSL/TLS over IMAP or POP; otherwise your emails are being sent in cleartext and can be read by outsiders. Also, turn on two-factor authentication, a security feature offered by the three big email services, Gmail, Yahoo, and Outlook (see "5 Email Myths Debunked," p. 82, for additional routine email-security measures). **Extreme fix:** People who truly need to guard their communications use PGP (Pretty Good Privacy) when they email each other. Every user has a pair of cryptographic keys, a public encryption key, and a private decryption one. The public key is widely distributed, while the private key is kept by the owner. A sender encrypts his or her note with the recipient's pub-

lic key, transforming it into gibberish. Since only the sender and receiver hold the keys, no one in the middle—including the email service provider—can decode the message. PGP doesn't hide the metadata, though, and everyone you communicate with has to be using PGP for it to work.

TECH: MOBILE DEVICES

TO DO: DELETE OLD APPS

There's no need to invent the ultimate citizen-surveillance device: It already exists, and it's called the smartphone. Police departments have been investing in IMSI catchers (that's short for International Mobile Subscriber Identity). These devices insert themselves between mobile devices and cell towers—the technology can be used to identify participants at a demonstration and even access their conversations. Hackers can build or buy the devices, as well. Additionally, law enforcement agencies can easily subpoena third-party companies for user data; in 2011 cellphone carriers responded to an astonishing 1.3 million demands for subscriber information. The companies handed over text messages, caller locations, and other information, in most cases without the knowledge of the user. Brick-and-mortar retailers are also making use of cellphone-location data: Some chains have started experimenting with using phones to track individual shoppers as they move through the store. And many mobile phone apps can transmit location data, contact lists, and calendar information back to their developers. Lose an unlocked phone and, of course, you give up access to your contact lists, emails, chats, and everything else that resides on your phone.

Routine fix: First, delete the apps you don't use—fewer apps means fewer robotic spies.

Extreme fix: Silent Phone can encrypt phone calls ($10/month, iOS and Android)—both parties need to be subscribers. There are also secure apps for IM chats and Web browsing. Prepaid, or burner, phones are relatively safe from snooping because they aren't tied to an account. And if you're worried about IMSI catchers at your next political rally, just leave your phone at home.

TECH: WI-FI

TO DO: USE ENCRYPTION

We all know that browsing on an unsecured network is just asking for someone armed with cheap network-analyzing software to tune in by vacuuming the 802.11 data packets flying between your machine and the Wi-Fi router. That can happen in Starbucks—or in your home. Last September a federal appeals court ruled that Google could be held liable for civil damages for eavesdropping on homeowners' Wi-Fi networks while using the company's camera-carrying Street View cars. Google says it was all a misunderstanding: The Wi-Fi data was being used to pinpoint precise locations where GPS signals were spotty.

Routine fix: Most wireless Internet access points come with WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access) to let you encrypt the messages between your computer and your access point. Use WPA if possible; it's the stronger technology. In addition to protecting your data, turning on encryption gives you legal protection against hackers under the Wiretap Act, which Congress passed in 1968 and last amended in 1986 through the Electronic Communications Privacy Act (ECPA). If you don't make any attempt to secure your data transmissions, the law assumes that your intention is to run a public network.

Extreme fix: Combine a virtual private network with the Tor bundle and you're as safe as you can be—well, almost. Want even better security? Don't use Wi-Fi at all. **PopMech**

Burner phones, prepaid devices that aren't tied to a specific account and allow people to switch numbers frequently, can be useful tools for the highly cautious.

License-plate readers (left), mounted atop patrol cars and along city streets, scan up to 1800 license plates per minute—keeping track of virtually every car on the road.

PHOTOGRAPHS BY ASSOCIATED PRESS (CAMERA), PHILIP FRIEDMAN (PHONE)