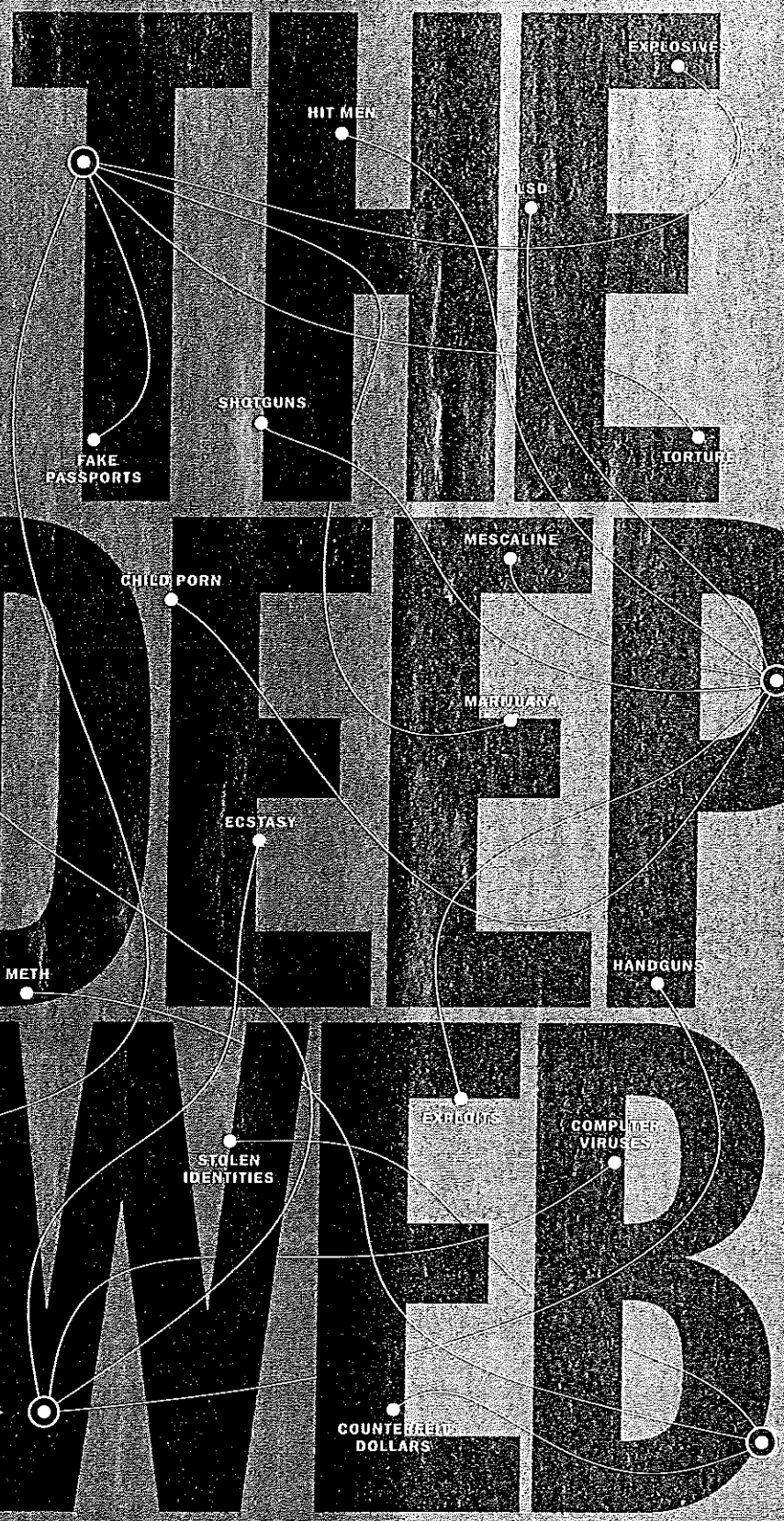
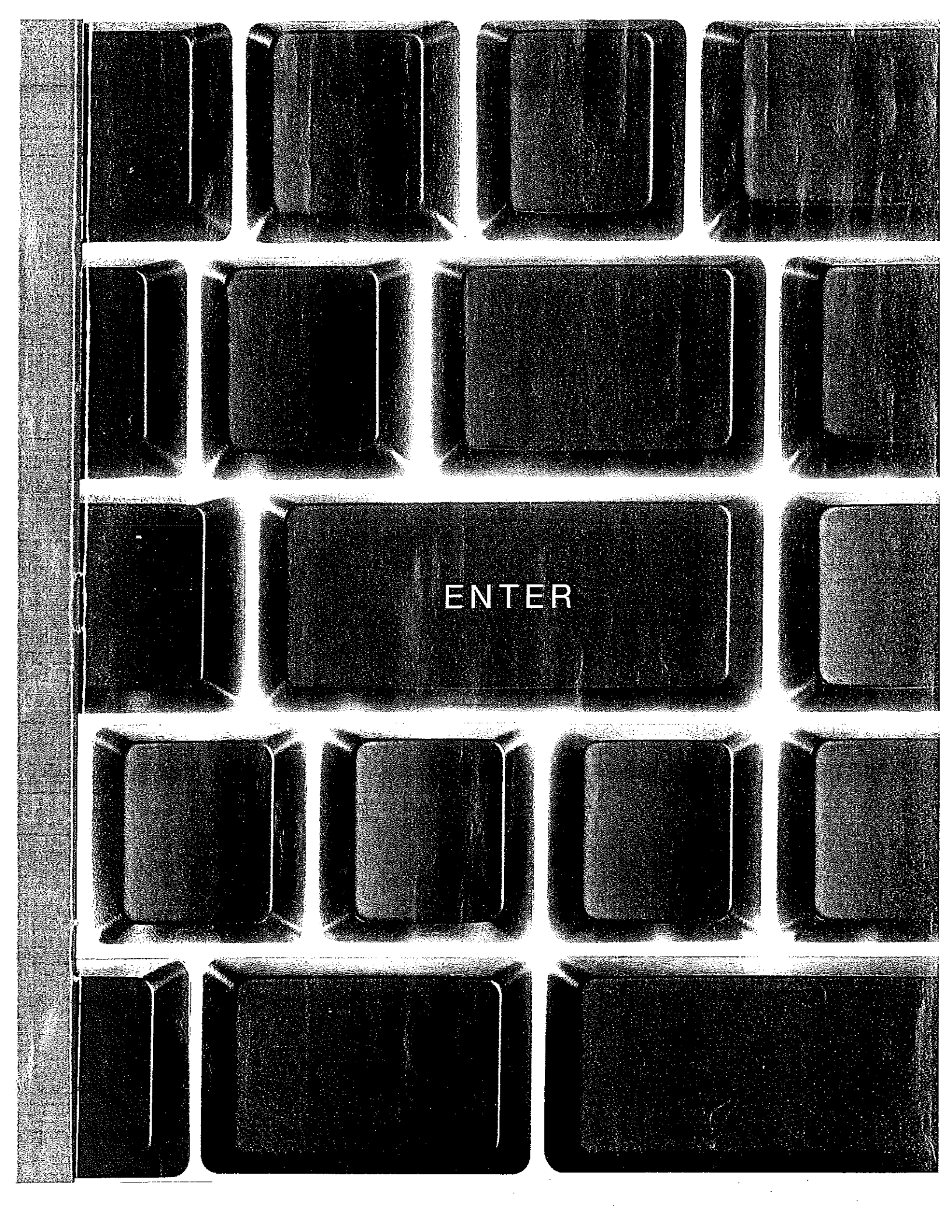
THE DEEP WEB



TEN YEARS AGO THE GOVERNMENT BUILT A TOTALLY PRIVATE, ANONYMOUS NETWORK. NOW IT'S A HAVEN FOR DRUGS AND CHILD PORNOGRAPHY BY LEV GROSSMAN AND JAY NEWTON-SMALL

Photo-illustration by Bartholomew Cooke for TIME


ENTER

ON

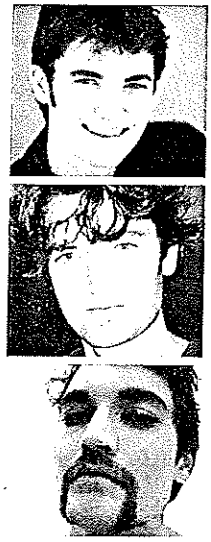
THE AFTERNOON OF OCT. 1, 2013, A TALL, slender, shaggy-haired man left his house on 15th Avenue in San Francisco. He paid $1,000 a month cash to share it with two housemates who knew him only as a quiet currency trader named Josh Terrey. His real name was Ross Ulbricht. He was 29 and had no police record. Dressed in jeans and a red T-shirt, Ulbricht headed to the Glen Park branch of the public library, where he made his way to the science-fiction section and logged on to his laptop—he was using the free wi-fi. Several FBI agents dressed in plainclothes converged on him, pushed him up against a window, then escorted him from the building.

The FBI believes Ulbricht is a criminal known online as the Dread Pirate Roberts, a reference to the book and movie *The Princess Bride*. The Dread Pirate Roberts was the owner and administrator of Silk Road, a wildly successful online bazaar where people bought and sold illegal goods—primarily drugs but also fake IDs, fireworks and hacking software. They could do this without getting caught because Silk Road was located in a little-known region of the Internet called the Deep Web.

Technically the Deep Web refers to the collection of all the websites and databases that search engines like Google don't or can't index, which in terms of the sheer volume of information is many times larger than the Web as we know it. But more loosely, the Deep Web is a specific branch of the Internet that's distinguished by that increasingly rare commodity: complete anonymity. Nothing you do on the Deep Web can be associated with your real-world identity, unless you choose it to be. Most people never see it, though the software you need to access it is free and takes less than three minutes to download and install. If there's a part of the grid that can be considered off the grid, it's the Deep Web.

The Deep Web has plenty of valid reasons for existing. It's a vital tool for intelligence agents, law enforcement, political dissidents and anybody who needs or wants to conduct their online affairs in private—which is, increasingly, everybody. According to a survey published in September by the Pew Internet & American Life Project, 86% of Internet users have attempted to delete or conceal their digital history, and 55% have tried to avoid being observed online by specific parties like their employers or the government.

But the Deep Web is also an ideal venue for doing things that are unlawful, especially when it's combined, as in the case of Silk Road, with the anonymous, virtually untraceable electronic currency Bitcoin. "It allows all sorts of criminals who, in bygone eras, had to find open-air drug markets or an alley somewhere to engage in bad activity to do it openly," argues Preet Bharara, U.S. attorney for the Southern District of New York, whose office is bringing a case against Ulbricht and who spoke exclusively to TIME. For 2½ years Silk Road acted as an Amazon-like clearinghouse for illegal goods, providing almost a million customers worldwide with $1.2 billion worth of contraband, according to the 39-page federal complaint against Ulbricht. The Dread Pirate Roberts, the Deep Web's Jeff Bezos, allegedly collected some $80 million in fees.



A pirate's life? *Friends describe Ross Ulbricht, a former Eagle Scout, as quiet and straitlaced*

Most people who use the Deep Web aren't criminals. But some prosecutors and government agencies think that Silk Road was just the thin edge of the wedge and that the Deep Web is a potential nightmare, an electronic haven for thieves, child pornographers, human traffickers, forgers, assassins and peddlers of state secrets and loose nukes. The FBI, the DEA, the ATF and the NSA, to name a few, are spending tens of millions of dollars trying to figure out how to crack it. Which is ironic, since it's the U.S. military that built the Deep Web in the first place.

TOR DE FORCE

THE STORY OF THE DEEP WEB IS A FABLE of technology and its unintended consequences. In May 1996, three scientists with the U.S. Naval Research Laboratory presented a paper titled "Hiding Routing Information" at a workshop in Cambridge, England. It laid out the technical features of a system whereby users could access the Internet without divulging their identities to any Web servers or routers they might interact with along the way. They called their idea "onion routing" because of the layers of encryption that surround and obscure the data being passed back and forth. By October 2003, the idea was ready to be released onto the Net as an open-source project called Tor (which originally stood for The Onion Router, though the acronym has since been abandoned). If the Deep Web is a masked ball, Tor provides the costumes. It was a highly elegant and effective creation so much so that even the people who built it didn't know how to break it.

In many ways Tor was less a step forward than a return to an earlier era. For much of the Internet's history, a user's online persona was linked only loosely, if at all, to his or her real-world identity. The Internet was a place where people could create new, more fluid selves, beginning with a handle or pseudonym. Through much of the 1990s, the Web promised people a second life. But over time—and in particular with the arrival of Facebook—our lives online have been tightly tethered to our off-line selves, including our real names. Now everywhere we go, we radiate information about ourselves—our browsing history, our purchases, our taste in videos, our social connections, often even our physical location. Everywhere but the Deep Web.

Why would the U.S. government fund the creation of such a system? Lots of reasons. The police could use it to solicit anonymous tips online, set up sting operations and explore illegal websites without tipping off their owners. Military and intelligence agencies could use it for covert communications. The State Department could train foreign dissidents to use it. Tor is currently administered by a nonprofit organization based in Cambridge, Mass., and sponsored by a diverse array of organizations including Google and the Knight Foundation. But as recently as 2011, 60% of its funding still came from the U.S. government.

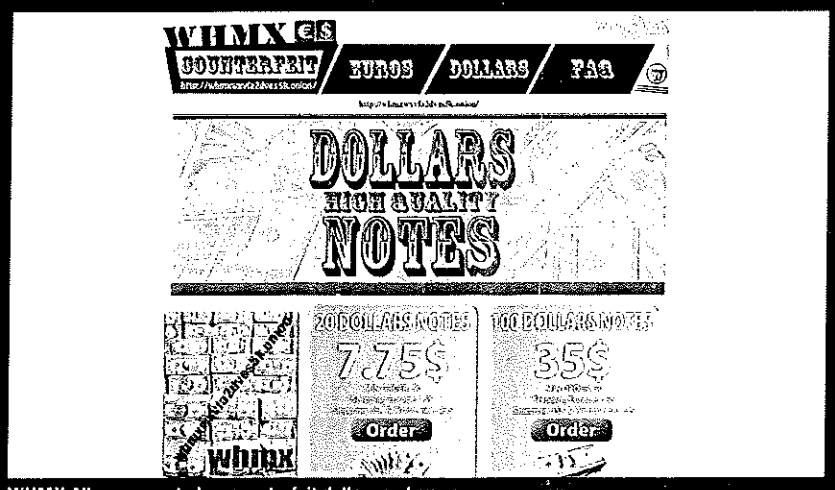
The corruption of the Deep Web began not long after it was built. As early as 2006, a website that came to be known as The Farmer's Market was selling everything

DARK MARKETS

Illicit sites like the now shuttered Silk Road find safe haven on the Deep Web and deal in everything from hard drugs to pornography

SILK ROAD Ross Ulbricht is accused of running the site that sold drugs and hacking software

UK PASSPORTS Sells forged documents, claiming to put passport numbers in a government database



WHMX Allows users to buy counterfeit dollars and euros

ULBRICHT: FROM TOP: POLARIS; FACEBOOK (2)

from marijuana to ketamine. It built up a clientele in 50 states and 34 countries before a DEA-led team brought it down in April 2012. The Deep Web isn't just a source for drugs: there is evidence that jihadists communicate through it and that botnets—massive networks of virus-infected computers employed by spammers—use it to hide from investigators. Even now, it's the work of a minute or two to find weapons or child pornography on the Deep Web. In August, the FBI took down Freedom Hosting, a company specializing in Deep Web sites, alleging that it was "the largest facilitator of child porn on the planet." Its owner, a 28-year-old named Eric Marques, is facing extradition from Ireland.

But Silk Road was different. For one thing, it was more discriminating: its terms of service forbade child pornography, stolen goods and counterfeit currency. For another, it didn't use dollars; it used bitcoins.

When Bitcoin appeared in 2009 it was a radically new kind of currency. It was introduced as a kind of fiscal thought experiment by someone known only as Satoshi Nakamoto, whose true identity is still a mystery. Bitcoin is both a payment system and a currency that is purely digital—it has no physical form. A bitcoin's worth is determined by supply and demand and is valuable only insofar as individuals and companies have agreed to trade it.

Bitcoins belong to an era in which trust in banks and government has been compromised. Users can transfer them from one digital wallet to another without banks brokering the transaction or imposing fees. The currency is completely decentralized—its architecture owes a lot to Napster's successor, BitTorrent—and is based on sophisticated cryptography. Bitcoin is essentially cash for the Internet, virtually anonymous and extremely difficult to counterfeit. The Farmer's Market was vulnerable because it left financial tracks in the real world. Silk Road didn't.

Like Tor, Bitcoin has entirely legitimate reasons for existing. As far as anyone can tell, it's primarily used for legal purposes—scores of businesses accept bitcoins now, including Howard Johnson, the dating website OKCupid and at least one New York City bar. But Bitcoin's digital slipperiness, when force-multiplied by the anonymity of the Deep Web, creates a potential platform for criminal transactions unlike anything the real or virtual world has ever seen. That potential was realized by the Dread Pirate Roberts.

JOHN GALT 2.0

ROSS ULBRICHT GREW UP IN TEXAS, AN Eagle Scout who went on to study physics at the University of Texas in Dallas. He was a fan of fellow Texan and libertarian Ron Paul; both studied the Austrian school of economics and the work of its father, Ludwig von Mises, who believed in unrestricted markets. Ulbricht earned a master's in materials science and engineering at Pennsylvania State University. Acquaintances describe him as bright and straitlaced. "He wasn't the center of conversation or the center of anything," says a friend who claims to have briefly dated him last year. "He kind of set himself in the background."

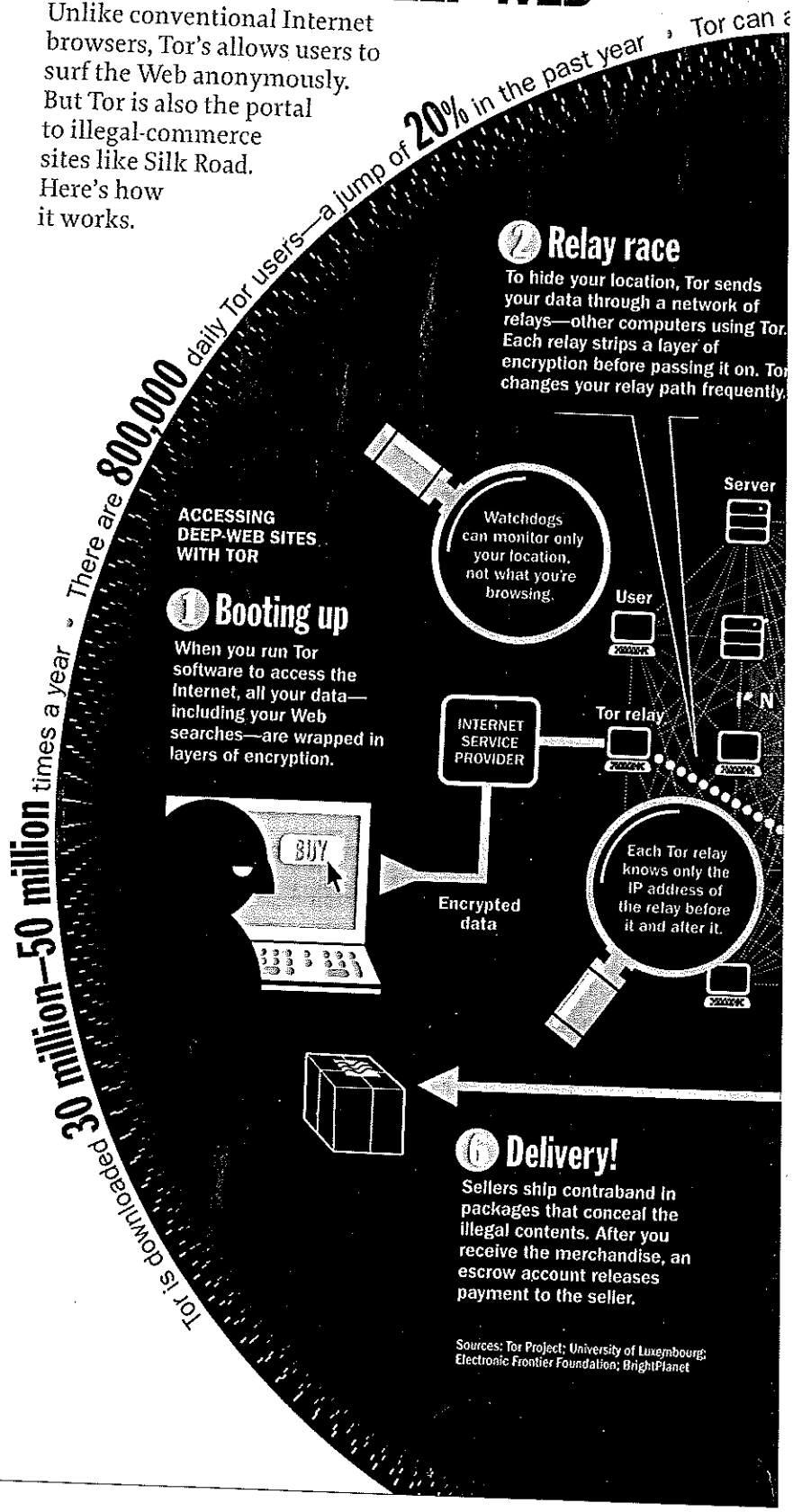
By the time he graduated, Ulbricht had become interested in the idea of the Internet as a venue for perfecting free markets. His greatest enemy—according to his LinkedIn profile—was the government. "The most widespread and systemic use of force is amongst institutions and governments, so this is my current point of effort," he wrote. "The best way to change a government is to change the minds of the governed, however. To that end, I am creating an economic simulation to give people a firsthand experience of what it would be like to live in a world without the systemic use of force."

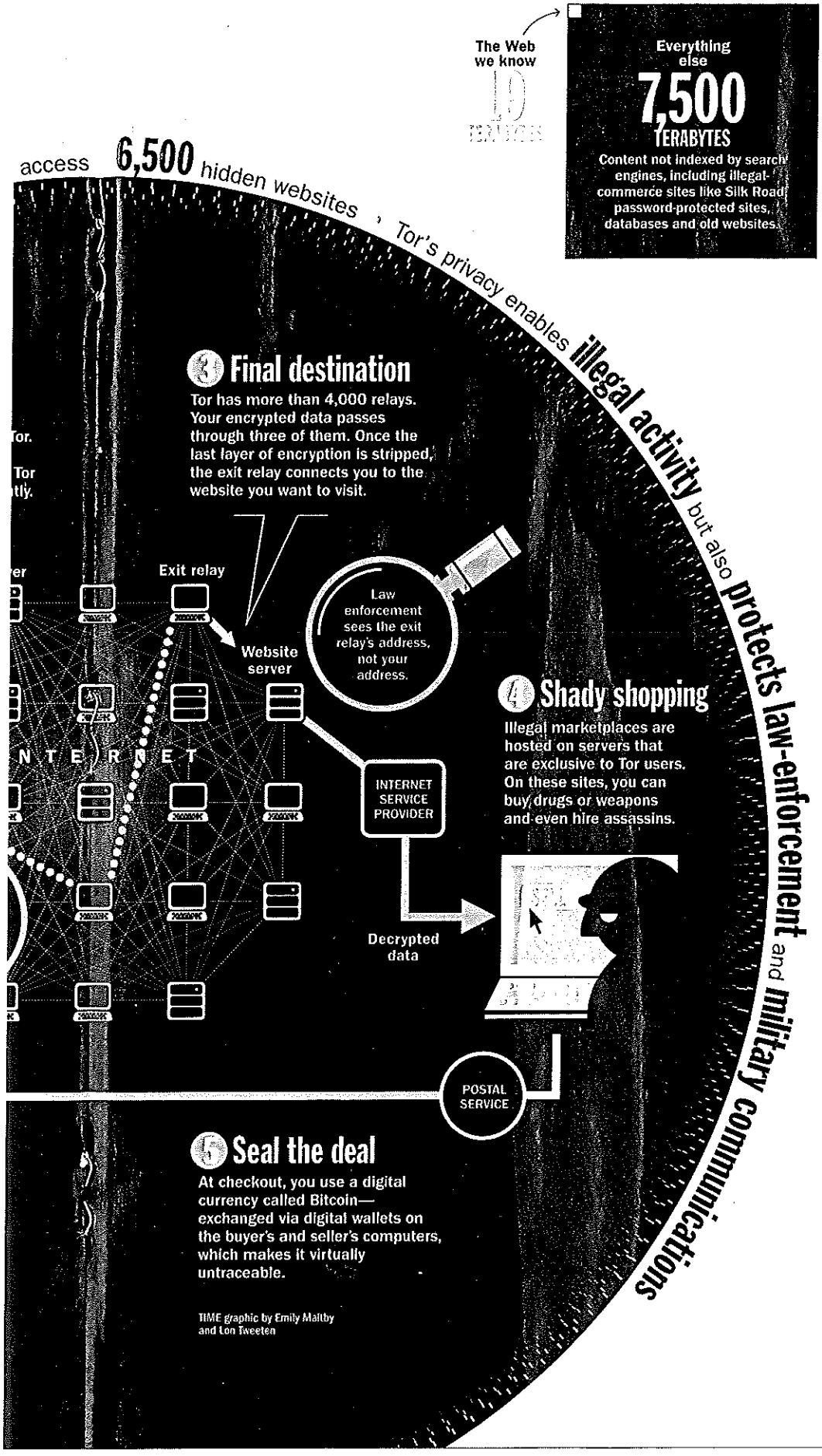
After graduating from Penn State in 2009, Ulbricht went to Sydney, Australia, to visit his sister. It was there, allegedly, that he began working on what would become Silk Road and transforming himself into the Dread Pirate Roberts. By then, drug dealers were already active on the Deep Web, but their businesses tended to fail for two reasons: the money changing hands was traceable, and it was difficult to build trust with clients. Roberts would solve both of those problems. The double layer of anonymity created by Tor and Bitcoin made the money virtually untraceable. To establish trust, Roberts looked to two temples of legitimate commerce for his ideas: Amazon and eBay.

He was a quick study. Users of Silk Road describe a sophisticated, full-featured experience complete with buyer and seller reviews and customer forums. "When deciding whether or not to go with a vendor, I read the feedback on their page and also ratings from a few months ago," says one Silk Road client, who declined to be identified. "I also go to the forums and read the seller's review thread, and depending on the substance, I'll go to an 'avenger's' thread, where people from the Silk Road

SURFING THE DEEP WEB

Unlike conventional Internet browsers, Tor's allows users to surf the Web anonymously. But Tor is also the portal to illegal-commerce sites like Silk Road. Here's how it works.





community post lab results for individual products." When transactions did go south, there was a dispute-resolution system. "Honestly it was like a candy store," says the user.

Products simply arrived by regular mail. "It generally looks like junk mail or information about moving here, or traveling there, or consultation stuff," the user explains. "Usually, when opening the package, you still won't know there are drugs in it unless you're looking for them." Silk Road's community had its own subculture, which skewed toward political outliers. "One memorable thread asked whether we were there for the drugs or the 'revolution,'" recalls the same user. "A lot of people answered 'came for the drugs, stayed for the revolution.'" Dread Pirate Roberts, or simply DPR, was hailed by Silk Road customers as an antiestablishment hero.

Silk Road launched in January 2011. Its existence was hardly kept a secret—with Tor making it possible to get in and out anonymously, why bother? Hiding would just have been bad for business. "It was basically an open thumbing of noses at law enforcement," Bharara says.

The FBI got its first glimpse of Ross Ulbricht that October. Someone named "altoid" had been promoting Silk Road in various chat rooms; then, in a Bitcoin forum, altoid posted an ad seeking an "IT pro in the bitcoin community" for "a venture-backed bitcoin-startup company," according to the complaint against Ulbricht. Ulbricht listed his real e-mail address as the contact for the position.

Ulbricht had left more clues for the feds. His Google+ account linked to some of the same sites and videos—including some from the Ludwig von Mises Institute—that the Dread Pirate Roberts mentioned. The FBI obtained records from Google that showed Ulbricht was accessing his Gmail account from San Francisco; the server through which Roberts accessed Silk Road showed an IP address corresponding to a San Francisco café. Ulbricht also posted a request for help with some computer code on a website for programmers, again under his own name. He hastily changed his user ID (to "frosty"), but the damage was done: that same code later turned up as part of the Silk Road site.

From there the thread becomes darker and more tangled. In January 2013, a Silk Road employee apparently stole bitcoins from users, then managed to get arrested

on another charge. Roberts, displaying a side investigators hadn't seen before, allegedly contracted with a Silk Road customer to have the employee tortured until he or she returned the bitcoins, then killed. This was the work not of a libertarian idealist but of a sociopath. Roberts was unaware that the hit man he was dealing with was an undercover FBI agent who had bought drugs on Silk Road as part of a sting operation. The agent sent Roberts faked photographic proof of the murder. Satisfied, Roberts wired $80,000 from an Australian money-transfer exchange.

According to the testimony of FBI agent Christopher Tarbell, who led the investigation, a Silk Road user in Canada began to blackmail Roberts, threatening to leak information about the site's clientele. Roberts responded by paying someone known online as "redandwhite" the sum of $150,000 in bitcoins to kill the blackmailer. (Roberts received photos of that killing too, but the Canadian police can't match it to any murder they're aware of.) In June 2013, Roberts ordered a set of fake IDs from redandwhite. Later that month, U.S. Customs opened a package from Canada containing nine fake IDs bearing Ulbricht's photo and birth date. The package also gave them Ulbricht's address.

The net was closing fast. By July, FBI hackers had tracked down one of Silk Road's servers, in a foreign country whose name has not yet been revealed, which gave them copies of all Roberts' e-mail plus transaction records dating to the site's launch. On July 26, agents from Homeland Security knocked on Ulbricht's door. He admitted that he'd been living under a false name.

The authorities got another break on July 31, when they raided the condo of a Seattle-area dealer who sold meth, coke and heroin through Silk Road under the handle Nod; they quickly flipped him as an informant. On Oct. 1, two years after they first spotted him, federal agents followed Ulbricht to the Glen Park library and arrested him. The FBI says it caught him red-handed with evidence on his laptop screen.

TRUTH AND CONSEQUENCES

MANY IN WASHINGTON ARE TROUBLED BY the fact that it took so much time and effort just to close one illegal website run by a would-be Walter White.

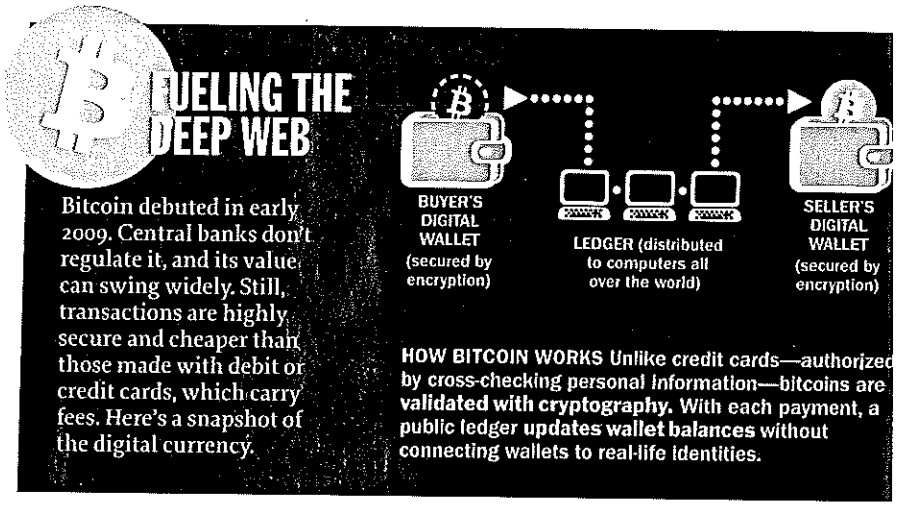
The FBI is policing an ever evolving Internet using static, often outdated laws. The Communications Assistance for Law Enforcement Act, which governs law enforcement's warrant process and is known as CALEA, was passed in 1994. "We're coming up next year on its 20th anniversary," says Marcus Thomas, former assistant director of the FBI's technology division, who now advises Subsentio, a firm that helps companies comply with CALEA. "It's in serious need of being updated to keep pace with the current environment."

Even leaving aside specialized tools like Tor, there are plenty of mainstream technologies that criminals can use to hide their activities: satellite phones, PIN messaging on BlackBerrys and even Apple iMessage, the instant-messaging service on iPhones and iPads. "The DEA got burned in April when it came out that we weren't able to capture iMessage on a wiretap," says Diana Summers Dolliver, a professor at the University of Alabama's department of criminal justice who previously worked at the Drug Enforcement Administration. "So of course all the bad guys went out and got iPhones and encrypted iMessage."

The FBI isn't trying to listen in on everything the way the NSA allegedly does; it's just looking to obtain legal search warrants under CALEA. But even that isn't as simple as it sounds. "First of all, even if you have an idea that they're using their computer to ill ends, you can't seize the computer for evidence," Dolliver says. "You have to have probable cause. So that's roadblock No. 1. Then, once you get ahold of their computer, it takes a lot of forensic work to figure out who the perps are." There are also many companies that have built their businesses specifically on providing their users with privacy and anonymity. Interest groups like the Center for Democracy and Technology argue that making new technologies CALEA-compliant stifles innovation and that building in back doors for law enforcement can make otherwise secure systems vulnerable to hackers.

For years the FBI has been working with other agencies on a proposal to update CALEA, which they finally submitted to the White House in April. The FBI won't comment on details, but generally speaking, the idea is not to force companies to divulge information, potentially compromising them technologically, but to increase fines on those that choose not to comply. If the arguments are reasonable, the timing is terrible: the Edward Snowden leaks began on June 5 and, almost at once, the idea of making electronic surveillance by the government easier became politically radioactive.

In 2012 the FBI established—jointly with the DEA, the ATF and the U.S. Marshals Service—the National Domestic Communications Assistance Center (NDCAC) in Quantico, Va. The center exists because—to quote from the appropriations bill that funds it—"changes in the volume and complexity of today's communications services and technologies present new and emerging challenges to



law enforcement's ability to access, intercept, collect, and process wire or electronic communications to which they are lawfully authorized." In essence, the NDCAC is a tech startup with at least $54 million in funding for the 2013 fiscal year that's focused on helping law enforcement penetrate areas of the Web that are currently unsearchable.

The FBI isn't the only agency that's worried about the Deep Web. The Senate Finance Committee is looking at beefing up the IRS' funding for dealing with virtual currencies and investigating potential tax shelters, Senate sources say. Bitcoin presents Washington with a whole set of regulatory challenges all on its own. Is Bitcoin a currency? (Under certain definitions, no, because it isn't legal tender issued by a country.) Is it a commodity? Should bitcoin traders be regulated as banks or wire services?

CRACKDOWN

THE INCARCERATION OF ROSS ULBRICHT started a spreading wave of arrests of suspected Deep Web dealers. On Oct. 8, police in Sweden arrested two men on charges of selling pot through Silk Road, and four more men were picked up in the U.K. the same day on drug charges. "These arrests send a clear message to criminals," said Keith Bristow, head of Britain's National Crime Agency. "The hidden Internet isn't hidden, and your anonymous activity isn't anonymous. We know where you are, what you are doing, and we will catch you."

It's not completely clear that that's true. One of the documents leaked by Snowden was an NSA presentation dated June 2012 titled "Tor Stinks." It described the difficulties the NSA has been having cracking Tor, and it said definitively, "we will never be able to de-anonymize all Tor users all the time." The Deep Web template that Ulbricht created remains technically sound. As one former Silk Road user puts it, "The dust has settled and everyone is kind of like 'Oh, well, time to order some more drugs.' We all knew it was coming." There are forum posts discussing the possibility of a reconstituted Silk Road, based on a backed-up version of the old site but with added security, that could launch on Nov. 5. "This will be where the action is once it's up and running," says the user.

Tor itself is left in the curious position of being funded by some parts of the federal government (including the State Department and the Department of Defense) while others (the FBI and the NSA) are trying to crack it. But even law-enforcement officials directly involved with the case hasten to clarify that they don't blame the technology itself for Silk Road. "There's nothing inherently wrong with anonymity on the Internet," U.S. Attorney Bharara says. "There's nothing inherently wrong with certain kinds of currency, like bitcoins. Just like there's nothing inherently wrong with cash. But it happens to be the case that ... it's also the thing that allows the drug trade to flourish. It allows money laundering to happen. It allows murder for hire to happen."

What's certain is that the need for Tor—or something like it—isn't going away. The Internet is becoming an increasingly unprivate place, where multibillion-dollar business plans are being built on companies' ability to observe and rapaciously harvest every last iota and fillip of consumer behavior. More and more, it falls to consumers themselves to say where the line is and to take control of their personal information.

What makes the Internet, and particularly the Deep Web, so hard to pin down is that it cuts across so many spheres that used to be strictly separate. It's private and public, personal and professional and political, all at the same time; it has a peculiar way of compressing all the formerly disparate threads of our lives into one single pipeline leading directly into our studies and bedrooms. It's virtually impossible for the law to tease those strands apart again. Right now we're trapped unpleasantly between two ideals, the blissful anonymity of the Net as it was first conceived and the well-regulated panopticon it is becoming. It's the worst of both worlds: the Deep Web provides too much privacy and the rest of the Web not enough.

Ulbricht himself currently has plenty of privacy. He's spending 20 hours a day alone in a cell in an Alameda County jail near Oakland, Calif. On Oct. 16 he hired a New York lawyer named Joshua Dratel, who has some experience with controversial cases. His past clients include several alleged terrorists. "He'll be pleading not guilty whenever he's arraigned on charges," Dratel told TIME. "He denies the charges right now, and he'll continue to deny [them]," he said. Perhaps inevitably, 20th Century Fox has already optioned the story of Silk Road from *Wired* magazine for a feature film.

Meanwhile, Ulbricht fills his days writing letters to friends and family and reading Patrick O'Brian's *Master and Commander*. He has no Internet access. He may, however, still have some of his pirate's treasure. On Oct. 25, Bharara announced that, after a prolonged hacking campaign, investigators had gained access to a cache of 122,000 of the Dread Pirate Roberts' bitcoins, worth over $24.9 million. But there may be many more millions out there. People may always be fallible and venal, but technology, at least for the time being, can still keep some of our secrets.

—WITH REPORTING BY JESSICA ROY AND LAURA STAMPLER/NEW YORK ■