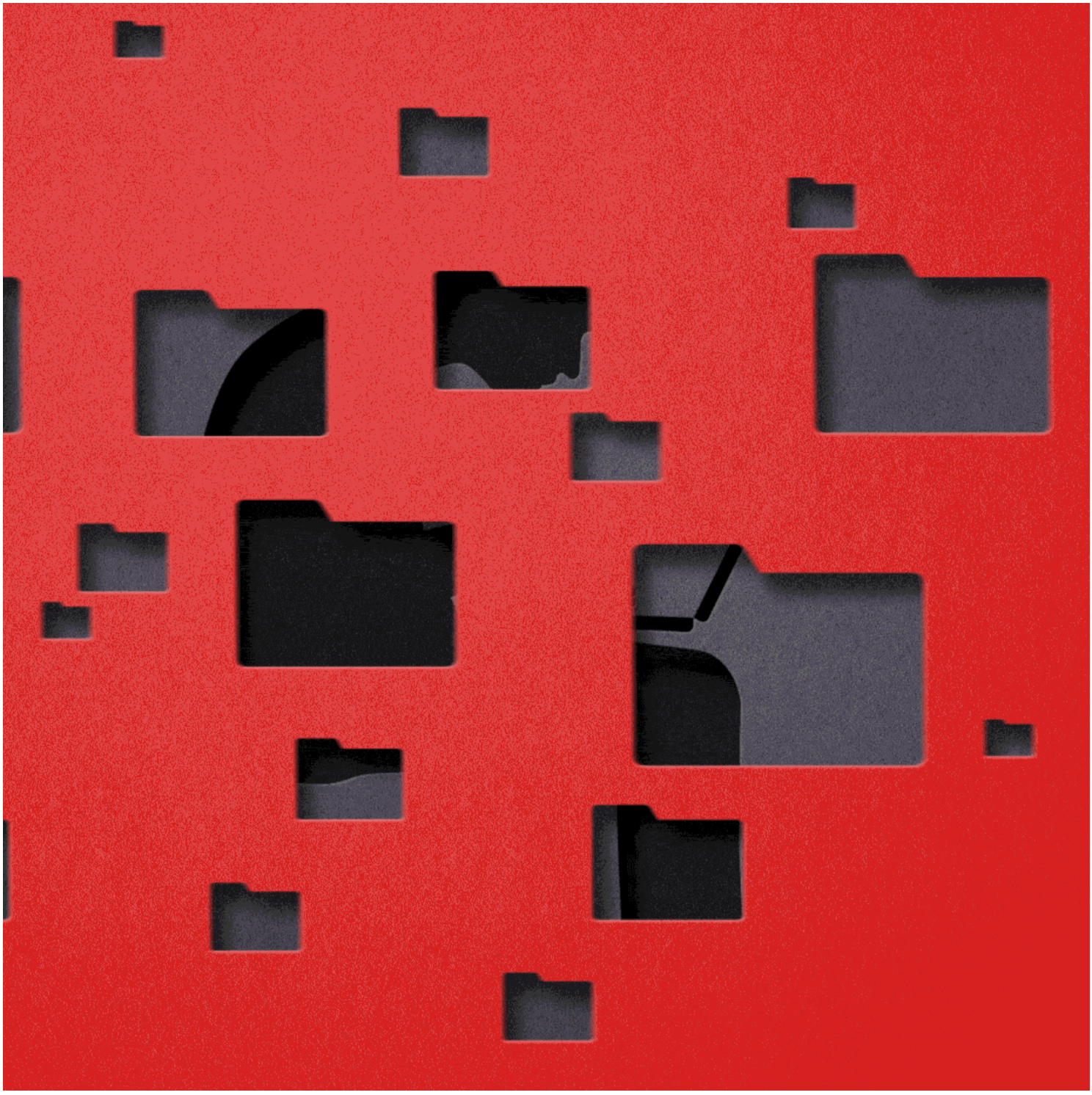
A REPORTER AT LARGE JUNE 13, 2022 ISSUE

THE SURREAL CASE OF A C.I.A. HACKER'S REVENGE

A hot-headed coder is accused of exposing the agency's hacking arsenal. Did he betray his country because he was pissed off at his colleagues?

By Patrick Radden Keefe

June 6, 2022



At the C.I.A., Joshua Schulte became so known for his temper that his colleagues gave him a nickname: the Nuclear Option. Illustration by Eiko Ojala

Listen to this story

0:00 / 1:13:52

To hear more, download the Audm app.

Nestled west of Washington, D.C., amid the bland northern Virginia suburbs, are generic-looking office parks that hide secret government installations in plain sight. Employees in civilian dress get out of their cars, clutching their Starbucks, and disappear into the buildings. To the casual observer, they resemble anonymous corporate drones. In fact, they hold Top Secret clearances and work in defense and intelligence. One of these buildings, at an address that is itself a secret, houses the cyberintelligence division of the Central Intelligence Agency. The facility is surrounded by a high fence and monitored by guards armed with military-grade weapons. When employees enter the building, they must badge in and pass through a full-body turnstile. Inside, on the ninth floor, through another door that requires badge access, is a C.I.A. office with an ostentatiously bland name: the Operations Support Branch. It is the agency's secret hacker unit, in which a cadre of élite engineers create cyberweapons.

"O.S.B. was focussed on what we referred to as 'physical-access operations,' " a senior developer from the unit, Jeremy Weber—a pseudonym—explained. This is not dragnet mass surveillance of the kind more often associated with the National Security Agency. These are hacks, or "exploits," designed for individual targets. Sometimes a foreign terrorist or a finance minister is too sophisticated to be hacked remotely, and so the agency is obliged to seek "physical access" to that person's devices. Such operations are incredibly dangerous: a C.I.A. officer or an asset recruited to work secretly for the agency—a courier for the terrorist; the finance minister's personal chef—must surreptitiously implant the malware by hand. "It could be somebody who was willing to type on a keyboard for us," Weber said. "It often was somebody who was willing to plug a thumb drive into the machine." In this manner, human spies, armed with the secret digital payloads designed by the Operations Support Branch, have been able to compromise smartphones, laptops, tablets, and even TVs: when Samsung developed a set that responded to voice commands, the wizards at the O.S.B. exploited a software vulnerability that turned it into a listening device.

The members of the O.S.B. "built quick-reaction tools," Anthony Leonis, the chief of another cyberintelligence unit of the C.I.A., said. "That branch was really good at taking ideas and prototypes and turning them into tools that could be used in the mission, very quickly." According to the man who supervised the O.S.B., Sean, the unit could be "a high-stress environment," because it was supporting life-or-death operations. (With a few exceptions, this piece refers to agency employees by pseudonyms or by their first names.)

But, while these jobs were cutting edge and—at least vicariously—dangerous, the O.S.B. was, in other respects, just like any office. There was a bullpen of cubicle workstations. A dozen or so people clocked in every day. “We were kind of known as the social branch,” another O.S.B. employee, Frank Stedman, recalled. The experience of O.S.B. engineers bore some resemblance to the Apple TV+ drama “Severance,” in that each morning they entered a milieu with its own customs and camaraderie—one sealed off from the rest of their lives. Because of national-security concerns, they couldn’t take work home, or talk with anyone on the outside about what they did all day. Their office was a classified sanctum, a locked vault. Like the crew of a submarine, they forged strong bonds—and strong antagonisms.

There was banter, plenty of it, much of it jocular, some of it juvenile. The coders were mostly young men, and they came up with nicknames for one another. One unit member, who got braces as an adult, became known as Train Tracks. When another brought food into the office one day, but didn’t share it with some members of the team, his colleagues bestowed a new handle: Dick Move. The group’s ultimate manager was a more senior C.I.A. official, named Karen, who acknowledged that the members could get “boisterous,” adding, “Folks could get a little loud, a little bit back and forth.” Some O.S.B. guys brought Nerf guns to work—not mere pistols but big, colorful machine guns—and they would occasionally shoot darts at one another from their desks. Sometimes people got carried away, and work was paused for some sustained bombardment. But Silicon Valley was known for tricking out offices with foosball tables and climbing walls, and it’s likely that the C.I.A. wanted to foster a loose culture on the hacking team, to help engineers remain innovative and, when necessary, blow off steam.

One of the Nerf gunfighters was Joshua Schulte—his real name. A skinny Texan in his twenties, he had a goatee and a shaved head. In what may have been a preëmptive gambit, Schulte gave himself the nickname Bad Ass, going so far as to make a fake nameplate and stick it on his cubicle. But others in the office called him Voldemort—a reference to the hairless villain in the Harry Potter books. Schulte and his colleagues worked on sophisticated malware with such code names as AngerQuake and Brutal Kangaroo. The hackers christened their exploits with names that reflected personal enthusiasms. Several programs were named for brands of whiskey: there was Wild Turkey, and Ardbeg, and Laphroaig. One was called McNugget. Though there was something dissonantly adolescent about naming highly classified digital hacking tools in such a fashion, it seemed harmless

enough: if the tools worked as planned, none of the code would ever be detected. And, if the target of an operation *did* discover that some nasty bit of malware had infiltrated her device, a silly name would offer no clue that it had been created by the United States government. Deniability was central to what the O.S.B. did.

On March 7, 2017, the Web site WikiLeaks launched a series of disclosures that were catastrophic for the C.I.A. As much as thirty-four terabytes of data—more than two billion pages' worth—had been stolen from the agency. The trove, billed as Vault 7, represented the single largest leak of classified information in the agency's history. Along with a subsequent installment known as Vault 8, it exposed the C.I.A.'s hacking methods, including the tools that had been developed in secret by the O.S.B., complete with some of the source code. "This extraordinary collection . . . gives its possessor the entire hacking capacity of the C.I.A.," WikiLeaks announced. The leak dumped out the C.I.A.'s toolbox: the custom-made techniques that it had used to compromise Wi-Fi networks, Skype, antivirus software. It exposed Brutal Kangaroo and AngerQuake. It even exposed McNugget.

"We just have a few more tragedies to report before we can get to the fun stuff."

Cartoon by P. C. Vey

In the days after this colossal breach became public, the C.I.A. declined to comment on the "authenticity or content of purported intelligence documents." Internally, however, there was a grim realization that the agency's secrets had been laid bare. "I was sick to my stomach," Karen, the O.S.B. supervisor, later recalled. "That information getting out into a forum like that can hurt people and impact our mission. It's a huge loss to the organization." Malicious code that had originated at the C.I.A. could now be attributed to the agency. And the potential fallout extended beyond the digital realm: a foreign target who had been hacked might now be able to identify the malware, determine when it had

been placed on a device, and even deduce which trusted member of the inner circle had engaged in betrayal. In the estimation of another senior C.I.A. official, Sean Roche, the leak amounted to "a digital Pearl Harbor."

But who could have stolen the data? In a statement, WikiLeaks suggested that the person who shared the intelligence wished "to initiate a public debate" about the use of cyberweapons. But WikiLeaks had also shown, quite recently, a willingness to be a mouthpiece for foreign intelligence services: in 2016, the site had released e-mails from the Democratic National Committee which had been stolen by hackers working on behalf of the Kremlin. Vault 7, some observers speculated, might also be the work of a hostile government. James Lewis, of the Center for Strategic and International Studies, told the *Times*, "A foreign power is much more likely the source of these documents than a conscience-stricken C.I.A. whistle-blower." Perhaps Russia was again the culprit. Or might it be Iran?

Given that the software exposed in Vault 7 had been maintained on a proprietary C.I.A. computer network that was not connected to the Internet, the spectre of espionage raised another alarming possibility. Might a foreign adversary have obtained "physical access"—smuggling a tainted thumb drive into the C.I.A.? Had the agency's own modus operandi been used against it?

As the intelligence community mobilized to identify the source of the leak, the federal government found itself in an awkward position—because Donald Trump, shortly before being elected President, had celebrated the hacking of Democratic officials, declaring, "I love WikiLeaks." Nevertheless, this new breach was perceived as such an egregious affront to U.S. national security that the Administration was determined to get to the bottom of it. The F.B.I. began an investigation, and agents worked around the clock. But an atmosphere of paranoia enshrouded the inquiry. One F.B.I. agent described how a C.I.A. officer who was approached for an interview reacted with reflexive suspicion, pointing out that anyone "can say they're an F.B.I. agent."

The Bureau was pursuing what it calls an "unsub"—or "unknown subject"—investigation. "A crime had been committed; we didn't yet know who had committed it," one of the lead investigators, Richard Evanchec, later testified. Fairly quickly, the agents ruled out a foreign power as the culprit, deciding that the unsub must be a C.I.A. insider. They zeroed in on

the classified computer network from which the data had been stolen—and on the agency employees who had access to that network. Among those who did were the O.S.B. hackers on the ninth floor of the agency's secret cyber installation in Virginia.

This was a befuddling prospect: the O.S.B. engineers devoted their professional lives to concocting clandestine digital weapons. Making public the source code would render their inventions useless. Why destroy your own work? As the F.B.I. interviewed members of the team, a suspect came into focus: Joshua Schulte. Voldemort. He had left the agency in November, 2016, and was said to have been disgruntled. He now lived in Manhattan, where he worked as a software engineer at Bloomberg. As Schulte was leaving the office one evening, Evanchec and another F.B.I. agent intercepted him. When they explained that they were investigating the leak, he agreed to talk. They went to a nearby restaurant, Pershing Square, opposite Grand Central Terminal. Schulte may not have realized it, but the other patrons seated around them were actually plainclothes F.B.I. agents, who were there to monitor the situation—and to intervene if he made any sudden moves. Schulte was amiable and chatty. But, when Evanchec looked down, he noticed that Schulte's hands were shaking.

Schulte was born in 1988 and grew up in Lubbock, Texas. He was the oldest of four boys; his father, Roger, is a financial adviser; his mother, Deanna, is a high-school guidance counsellor. Schulte was a bright child, and in elementary school he was fascinated when one of his teachers took apart a computer in front of the class. By the time he was in high school, his parents told me, he was building computers himself. "Some people are born with certain talents," Deanna said. While Schulte was studying engineering at the University of Texas at Austin, he did an internship at I.B.M., and another at the N.S.A. On a blog that he maintained in college, he espoused libertarian views. He was a devotee of Ayn Rand, and came to believe that, as he put it, "there is nothing evil about rational selfishness." He also had a certain intellectual arrogance. "Most Americans, most people in general, are idiots," he wrote in 2008.

"I don't want a 'Big Brother' constantly looking over my shoulder," Schulte once wrote, and his libertarianism might have seemed difficult to square with a career in intelligence. Kavi Patel, who knew Schulte in junior high and became close friends with him in high school, recalled, "He was always a huge Ron Paul guy," adding that Schulte was drawn to "the people who say the government is infringing on our rights." Nevertheless, according to

Schulte's parents, his dream was to work for the government. "He never talked about the private sector at all," Deanna told me, explaining that he was motivated by patriotism. "I think he was very proud to serve his country." In a blog post, Schulte argued that "privacy and individual security are antithetical," and that "increasing one ultimately decreases the other." By the time he finished college, in 2011, he had been hired by the C.I.A. Many people regarded the N.S.A. as the premier government employer for coders and hackers, but the C.I.A.'s hacking unit may have offered more palpable proximity to exciting operations on foreign soil. Schulte wanted to fight terrorists.

Like drone pilots who destroy villages in Afghanistan from an air-conditioned trailer in Nevada, the engineers of the O.S.B. experienced an uncanny incongruity between the safety of their surroundings and the knowledge that their work supported high-stakes covert operations abroad. "We were very mission-focussed," Jeremy Weber recalled. "But, you know, we had fun at work, too." Schulte proved to be a capable programmer, and in 2015 he was granted a special distinction when he was made a system administrator for the C.I.A.'s developer network, or DevLAN. Now he could control which employees had access to the network that held the source code for the group's many projects. Being a system administrator was regarded, Weber said, as "a privileged position." Schulte made good friends at work; he became particularly close with another member of the O.S.B. team, named Michael. They played video games together after hours, or went to the gym.

But Schulte could also be abrasive. "Josh was very opinionated on the way things should be done," Weber observed. "So he had some rough edges." In particular, if Schulte felt wronged in some way, he had a pronounced tendency to overreact. One day at work, he shot a rubber band at Michael, and Michael returned fire. "This went back and forth until late at night," Michael recalled. "He trashed my desk, I trashed his desk." The conflict escalated until both men were throwing punches.

Schulte could get "a little off the hinge," Sean remembered. At one point, agency officials decided to assign a contractor a project, Almost Meat, that was based in part on Schulte's code. "Josh was offended," Weber recalled. He protested that his hard work would be handed to a third party, then sold back to the government at a markup. He threatened to file a complaint with the C.I.A.'s inspector general, claiming "fraud, waste, and abuse." Frank Stedman, who worked on Almost Meat, felt that the episode illustrated Schulte's

tendency to react with a “disproportionate response.” The man known as Bad Ass and Voldemort accrued another office nickname: the Nuclear Option.

Schulte using a contraband cell phone while incarcerated at the Metropolitan Correctional Center, in Manhattan. U.S. Trial Exhibit

Schulte had been on the job for about three years when a new programmer named Amol joined the O.S.B. He sat near Schulte, and they were partnered on a project code-named Drifting Deadline. According to Weber, Amol and Schulte "didn't get along, and from the get-go." Initially, people ribbed Amol because he behaved in a professional manner that was at odds with the prevailing frat-house vibe. Schulte liked to shoot Amol with his Nerf gun. As Amol grew more accustomed to the O.S.B.'s raucous culture, he started fighting back. He would collect Schulte's Nerf darts and stash them behind his desk. He began trolling others in the office, maligning their skills as coders and devising his own cruel nicknames. He referred to Schulte as Bald Asshole. Amol was heavy, and Schulte reciprocated by making fun of his weight. Their bickering intensified.

In October, 2015, Amol complained to Sean, the hacking-unit supervisor. "I have had enough of Schulte and his childish behavior," he wrote. "Last night, he shot me in the face with his nerf gun and it could have easily hit me in the eye." Schulte also wrote to Sean, saying that Amol was "very derogatory and abusive to everyone." According to Schulte, Amol had told him, "I wish you were dead," "I want to piss on your grave," and "I wish you'd die in a fiery car crash." Such rhetoric, Schulte noted, "does little to foster collaboration."

Weber subsequently confirmed that Amol had indeed said some of these things. But he pointed out that Amol had done so only after protracted arguments with Schulte, and that the attritional verbal combat Schulte seemed to favor could "exhaust" a person. In March, 2016, the discord between the two hackers reached a new level, when Schulte lodged a formal complaint with security officials at the C.I.A., reporting that Amol had told him, "I

wish you were dead, and that's not a threat, it's a fucking promise." Schulte characterized this as a credible death threat that had left him fearing for his life. He suggested that Amol was "upset and unstable," and possibly bipolar.

Schulte felt that his superiors weren't taking his accusations seriously. He neither liked nor respected Karen, his ultimate boss, referring to her as a "dumb bitch." One C.I.A. security official responded to the dispute by saying that he couldn't play "high school counselor," which only exacerbated Schulte's anger. Schulte escalated the matter by complaining to the director of the cyberintelligence division, Bonnie Stith—an agency veteran who oversaw several thousand employees. One might suppose that she had more pressing matters to contend with, but she offered to sit down with Schulte and Amol and try to broker peace. Initially, Schulte refused, saying that he was afraid to be in the same room with Amol. But she insisted, and at the meeting she urged both men to consider the "honor" of being C.I.A. employees, and to remember their obligations to their country. Amol, she thought, seemed embarrassed to have been hauled before the school principal. Stith decided that the coders should be physically separated. "Our nation depended on us," she pointed out later. "I needed them to be focussed."

Schulte was furious to learn that he had to switch desks. He said that he would relocate only if his managers issued the directive in writing. So they did. Even then, he refused to fully move. He didn't like the new location. It had no window. It was an "intern desk," he scoffed; Amol, meanwhile, had been " 'promoted' to a better desk," leaving Schulte "exposed to questions and ridicule about why I was demoted."

Up to this point, though Schulte could be vexing and obstreperous, he was working within the broad bureaucratic parameters of the agency. Others might have found his vendetta against Amol irrational, but he had confined it to traditional channels, pushing his appeal up the chain of command. Now he embarked on a more decisive escalation, concluding, as he later explained, that "since the Agency wouldn't help me, perhaps the state would." Citing fears for his safety, Schulte filed for a restraining order against Amol in Virginia state court.

This was a startling departure from normal conduct for the C.I.A. The agency has an estimated twenty thousand employees, and, because of the sensitivity of its work, it enjoys remarkable autonomy within the federal government, sometimes appearing to operate as a

self-governing fief. The notion of allowing an internal squabble to spill into the unclassified realm was anathema. "It was *so* unusual to have agency employees in a local court," Stith later said.

Amol was obliged to appear at an open hearing at a Loudoun County courthouse. Inside the agency, a security organ known as the Threat Management Unit was activated, and a decision was made to separate the warring O.S.B. programmers even further, moving Schulte to a different branch altogether, on the eighth floor. Schulte fired off an intemperate e-mail: "I just want to confirm this punishment of removal from my current branch is for reporting to security an incident in which my life was threatened." Of course, it was also possible to read this relocation as a logical bureaucratic response to the restraining order that Schulte had obtained, which compelled Amol to avoid any contact with him—even crossing paths in the hallway.

Leonard Small, an official from the agency's Office of Security, later said that "Josh's escalating behavior" kept "going on and on." In an e-mail to Small, Schulte threatened to go public, saying that a lawyer he had spoken to had suggested, "An article titled 'C.I.A. PUNISHES EMPLOYEE FOR REPORTING OFFICE DEATH THREATS' would be an article that the media would be very interested in." Schulte hadn't yet "proceeded with this option," he said, because he was "hoping there is an alternative."

Others in the O.S.B. expressed frustration with Schulte's refusal to drop the matter. At one point, Stedman observed, "The boy needs to learn how to take his medicine." Nobody believed that Amol had posed a genuine threat to Schulte's life. Stedman later declared that "the whole writeup is bullshit and exaggerated," and read like "a fictional narrative." As an intelligence professional trained in the art of threat assessment, he considered it "insulting" that Schulte thought any of them might fall for such a ruse.

Next, Schulte appealed to several of the most senior officials at the C.I.A., including Meroë Park, the executive director. "I know you don't deal with personnel issues and likely won't spend much time on this, but management's abuse of power and consistent retaliation against me has forced me to resign," he wrote, on June 28, 2016. Schulte hung on a little longer, but by November he was gone. At Bloomberg, he would make more than two hundred thousand dollars a year—a significant increase from his government salary. Though he was legally bound to protect the confidentiality of his C.I.A. work, he could tell

people he had been at the agency, and he discovered that in the private sector this conferred a certain cachet. Reflecting on Schulte's good fortune, Stedman noted that sometimes "good things happen to bad people."

Before Schulte's departure, there had been one final fracas. Schulte was, in his own telling, trying "to make the best of my situation and move forward," but after relocating to the eighth floor he attempted to work on Brutal Kangaroo—only to find that his access had been denied. "Imagine my shock," he later recalled, noting that Brutal Kangaroo had been *his* project; he felt a huge proprietary investment in the program. Schulte consulted the audit logs on the system, and determined that Weber had stripped him of his access. Weber later explained that his reasoning had been simple: in Schulte's new branch, he "was going to be working on new projects," and therefore wouldn't need access to the old ones. But Schulte saw it as retribution. He had developed a special resentment for Weber. At the Loudoun County court hearing on the restraining order, Weber had shown up—as a show of solidarity with Amol. Schulte regarded Weber as a bureaucratic toady, Karen's "loyal pawn." Weber, he felt, "had played politics to overthrow me from my own project."

And so Schulte, without asking for authorization, reassigned himself access to his old project. When his managers learned of this, they were so alarmed that they stripped Schulte of his administrator privileges. Weber later said of Schulte's transgression, "The agency exists in a world of trust. We are granted access to classified information, and we are trusted to only use that information for the expressed reasons we're given access to it." If you can't "trust the person that you're working with," he pointed out, you're in trouble. (Schulte has disputed Weber's account of these events.)

"Oh, yeah? Would a 'never spontaneous' person order two pairs of final-sale chinos online?"

Cartoon by Hartley Lin

Official secrecy is a slippery phenomenon. Organizations such as WikiLeaks espouse an absolutist commitment to transparency, but, in a world where genuinely bad actors exist and the interests of nation-states don't always align, most Americans would acknowledge the need for some degree of secrecy, as a prerogative of statecraft and national defense. Nevertheless, the U.S. system of classification has grown wildly out of control. In 1989, Erwin Griswold, who had argued the Pentagon Papers case on behalf of the government—and was therefore hardly a friend to leakers—published an op-ed in the

Washington *Post* in which he maintained that there were *too many* state secrets. Classification had evolved into a bureaucratic reflex, he pointed out, and "the principal concern of the classifiers is not with national security, but rather with governmental embarrassment." More recently, the 9/11 Commission concluded that overclassification, far from keeping the country safer, actually jeopardizes national security, by inhibiting the sharing of information among government agencies.

Before Daniel Ellsberg leaked the Pentagon Papers, in 1971, he had photocopied seven thousand pages by hand. (He enlisted his teen-age son to help.) Digital technology has allowed such leakers as Edward Snowden and Chelsea Manning to purloin much vaster reams of data with significantly greater ease. "I would come in with music on a CD-RW labelled with something like 'Lady Gaga,' erase the music then write a compressed split file," Manning once boasted, recalling how she lip-synched to Gaga's "Telephone" while "exfiltrating possibly the largest data spillage in American history."

Snowden and Manning were not seeking to blow the whistle on any one particular policy, in the manner that Ellsberg was; theirs was a more generalized disaffection, and the troves of data that they exposed were indiscriminate, comprising not just instances in which U.S. authorities had engaged in appalling, illegal conduct but also instances in which they had behaved appropriately. One could debate whether the term "whistle-blower" is adequate to describe someone who leaks gigabytes of data. But it's clear that these wholesale digital disclosures are themselves an unintended consequence of overclassification. The number of Americans who possess a security clearance has swelled to more than five million, because classification has swathed in secrecy so many functions of defense and intelligence work. Given the expanding universe of classified documents, the widening pool of professionals with access to them, and the increasing ease with which data can be downloaded and filched, further jumbo leaks appear inevitable.

Unlike other prominent digital leakers, Schulte did not seem like an ideological whistle-blower. Ayn Rand fanboys are not exactly famous for their doctrinal consistency, and Schulte's concerns about "Big Brother" don't appear to have occasioned much soul-searching in the years he spent building surveillance weapons for a spy agency. On an anonymous Twitter account that Schulte maintained, he reportedly expressed the view (in a since-deleted tweet) that Chelsea Manning should be executed. Weber recalled Schulte saying that Snowden deserved the same. Could it be that Schulte had leaked the C.I.A.'s

digital arsenal not because of any principled opposition to the policies of the U.S. government but because he was pissed off at his colleagues? There are prior examples of C.I.A. employees who have been driven to betray their country out of a sense of professional grievance: after an agency officer named Edward Lee Howard was fired, in 1983, because he had lied about drug use and other minor transgressions during a polygraph exam, he began feeding the K.G.B. sensitive intelligence; when the agency discovered the breach, Howard fled to Russia, where he lived until his death, in 2002. After Ellsberg made the moral decision to leak the Pentagon Papers, it took him weeks of complicated work to make good on that objective. But with digital technology the window between impulse and consummation shrinks considerably, and, as everyone who worked with Josh Schulte knew all too well, when he was mad he had poor impulse control.

Even as F.B.I. investigators pinpointed Schulte as the prime suspect, their work was frustrated by the pageantry of overclassification. WikiLeaks had posted the Vault 7 tools on the Web, where anyone could see them, but officially the C.I.A. and the F.B.I. maintained that the documents remained classified. As a result, only investigators who held the necessary security clearances were permitted even to access WikiLeaks to see what had been stolen. F.B.I. officials were so nervous about visiting the Web site using Bureau computers or Internet connections (thereby possibly exposing their *own* networks to a cyber intrusion) that they dispatched an agent to purchase a new laptop and visit the Web site from the safety of a Starbucks. Once the Vault 7 materials had been downloaded from the Internet, the laptop itself became officially classified, and had to be stored in a secure location. But the evidence locker normally used by agents, which held drugs and other seized evidence, wouldn't do, because it was classified only up to the Secret level. Instead, the investigators stored the laptop in a supervisor's office, in a special safe that had been certified to hold Top Secret documents—even though anyone could go to the Internet to see the materials that were on it.

Soon after the F.B.I. began its investigation, agents placed Schulte under surveillance, and they learned that he was about to leave for Mexico. Edward Snowden had fled to Hong Kong and then to Russia, where he remains, beyond the reach of U.S. authorities. Faced with the possibility that Schulte might abscond in similar fashion, investigators made their move, with Agent Evanchec stopping him as he left work at Bloomberg and taking him to Pershing Square. It had emerged that when Schulte left the C.I.A. he had not returned his special black government passport, which assured the holder official status when travelling

abroad. Schulte eventually acknowledged that he still had the passport, but maintained that the trip to Mexico was simply a spring-break excursion with his brother. (Roger Schulte told me that the brothers had purchased round-trip tickets for a short visit to Cancún.)

The investigators had a warrant to search Schulte's apartment, so they all went together to his building, on Thirty-ninth Street. It was full of computer equipment. When F.B.I. agents obtained a warrant for Schulte's search history from Google, they discovered that, starting in August, 2016—when he was preparing to leave the C.I.A.—he had conducted thirty-nine searches related to WikiLeaks. In the hours after WikiLeaks posted Vault 7, he searched for "F.B.I.," and read articles with such titles as "F.B.I. Joins C.I.A. in Hunt for Leaker." For a guy who was a supposed expert in information warfare, Schulte seemed shockingly sloppy when it came to his own operational security. Even so, the F.B.I. hadn't found a smoking gun. It had amassed circumstantial evidence tying Schulte to the Vault 7 leak, but it hadn't found any record of him transmitting data to WikiLeaks—or, indeed, any proof that the secret files had ever been in his possession.

Schulte was not under arrest, so he got a room at a hotel while the search of his apartment continued. The F.B.I. seized his computer hardware, for forensic analysis. When computer scientists at the Bureau examined Schulte's desktop, they discovered a "virtual machine"—an entire operating system nested within the computer's standard operating system. The virtual machine was locked with strong encryption, meaning that, unless they could break the code or get the key from Schulte—both of which seemed unlikely—they couldn't access it. But they also had Schulte's cell phone, and when they checked it they discovered another startling lapse in operational security: he had stored a bunch of passwords on his phone.

One of the passwords let the investigators bypass the encryption on the virtual machine. Inside, they found a home directory—also encrypted. They consulted Schulte's phone again, and, sure enough, another stored password unlocked the directory. Next, they found an encrypted digital lockbox—a third line of defense. But, using encryption software and the same password that had unlocked the virtual machine, they managed to access the contents. Inside was a series of folders. When the investigators opened them, they found an enormous trove of child pornography.

When the news broke that Schulte was a suspect in the Vault 7 leak, Chrissy Covington, a d.j. and a radio personality in Lubbock who had attended junior high

school with him, took to Facebook to express her surprise. “The gravity of his crimes? OMG. Y’all,” she wrote, in a group chat with several classmates who had also known Schulte. Covington and Schulte had been friendly; as teen-agers, they chatted on AOL Instant Messenger. She was surprised to learn not only that he might be the leaker but also that the C.I.A. had given him a job in the first place. “How could you hire *Josh Schulte*?” she said when I spoke to her recently. “007 he’s not.” Schulte had always struck Covington as an “oddball,” but mostly harmless. On Facebook, however, she started to hear from classmates who shared unpleasant memories of Schulte crossing boundaries and making others uncomfortable. Several former classmates recalled to me that Schulte was infamous for drawing swastikas in school, and that, on at least one occasion, he did so on the yearbook of a Jewish student.

Other classmates recalled sexually inappropriate behavior. One woman told me that he had repeatedly exposed his penis to students when they were both in the junior-high band. “He would try and touch people, or get people to touch him—that was a daily occurrence,” she said. She loved music, but she was so intent on getting away from Schulte that she asked her parents to let her quit the band. She was too uncomfortable to explain to her parents exactly what had transpired. “It’s hard to put it into words,” she recalled. “You’re twelve. It’s just ‘Hey, this kid is super gross, and it makes me want to not be part of this school right now.’ ” Her parents, not grasping the gravity of what had happened, insisted that she remain in the band. “I was traumatized,” she told me. I also spoke to a friend of the woman, who remembered her recounting this behavior by Schulte at the time. A third woman told me that Schulte and some of his friends got in trouble at school after trying to stick their hands into her pants while she slept on the bus during a field trip. Schulte, she said, took revenge by sending her an AOL message loaded with a virus, destroying her computer. He boasted about the hack afterward, the woman said.

Schulte’s friend Kavi Patel acknowledged that Schulte would “draw swastikas all over the place.” He wasn’t anti-Semitic, Patel contended; he just relished getting a rise out of people. He recalled Schulte telling him, “I don’t really care one way or the other, but it’s fun to see the shock on people’s faces.” Patel was also in the junior-high band. When I asked him if he remembered Schulte exposing himself, he said that he never witnessed it, but had heard about it happening “two or three times.” According to Patel, Schulte seemed to confirm it to him on one occasion: “I was, like, ‘Dude, did you do this?’ And he was, like, ‘Heh, heh.’ ” Patel added, “It’s not something that’s out of his character. At all.” (Presented with these

allegations, several attorneys who have represented Schulte had no comment. Deanna recalled learning that Joshua had drawn a swastika in his notes for a lesson on the Second World War, but she and Roger said that they were not aware of other incidents involving swastikas or the junior-high band. They dispute the classmate's recollection of the incident on the school bus.)

"I'll be back at the end of the year with a 1099."

Cartoon by Liana Finck

When Schulte was in college, he argued on his blog that pornography is a form of free expression which "is not degrading to women" and "does not incite violence." He went on, "Porn stars obviously enjoy what they do, and they make quite a bit of money off it." Of course, some women are coerced into pornography, and if you mistake the simulated enjoyment in a porn performance for the real thing then you don't understand much about the industry. But more to the point: child pornography is not free expression; it's a crime. After Schulte realized that the illicit archive had been discovered, he claimed that the collection—more than ten thousand images and videos—didn't belong to him. In college, he had maintained a server on which friends and acquaintances could store whatever they wanted. Unbeknownst to him, he contended, people had used the server to hide contraband. He "had so many people accessing it he didn't care what people put on it," Roger Schulte told the *Times*.

But, according to the F.B.I., as agents gathered more evidence they unearthed chat logs in which Schulte conversed about child pornography with fellow-enthusiasts. "Where does one get kiddie porn anyways?" Schulte asked, in a 2009 exchange. This was another instance in which Schulte seemed recklessly disinclined to cover his tracks. His Google search history revealed numerous queries about images of underage sex. In the chat logs, people seeking or discussing child pornography tended to use pseudonyms. One person Schulte interacted with went by "hbp." Another went by "Sturm." Josh's username was "Josh." At one point, he volunteered to grant his new friends access to the child-porn archive on his server. He had titled it /home/josh/http/porn. Sturm, taken aback, warned Schulte to "rename these things for god's sake."

When F.B.I. investigators searched Schulte's phone, they found something especially alarming: a photograph that looked as though it had been taken inside the house in Sterling, Virginia, where he had lived while working for the C.I.A. The photograph was of a woman who looked like she was passed out on the bathroom floor. Her underwear appeared to have been removed and the hand of an unseen person was touching her genitals. State investigators in Loudoun County subsequently identified the woman and interviewed her. She has not been publicly named, but she told them that she had been

Schulte's roommate and had passed out one night, with no memory of what had happened. The encounter in the photograph was not consensual, she assured them. According to subsequent legal filings, the investigators concluded, after consulting the victim, that the hand in the photograph belonged to Schulte.

On August 24, 2017, at 5:30 A.M., a dozen armed federal agents hammered on the door of his apartment in Manhattan, startling him awake. Once inside, they bellowed, "Turn around and put your hands behind your back!" According to an account written by Schulte, he was led "like a prized dog" into the federal courthouse in lower Manhattan, where he was cuffed and shackled, then turned over to the U.S. Marshals. At this point, the F.B.I. and federal prosecutors had been investigating Schulte's possible role in the Vault 7 leak for five months, but they still hadn't indicted him. Instead, they now charged him with "receipt, possession, and transportation" of child pornography. Schulte pleaded not guilty. When he heard that the government was pushing to keep him detained pending trial, his stomach dropped. "The crime I am charged with is in fact a non-violent, victimless crime," he objected, displaying an obdurate heedlessness when it comes to how child pornography is made. (In a recent court filing, Schulte asserted that he has been "falsely accused" of acquiring child pornography.)

A judge ultimately ruled that Schulte could be released on bail, on the ground that he posed no immediate threat to society. But his release came with stringent conditions. He would be under house arrest, unable to leave his apartment except for court dates. And he could not access the Internet. Schulte bridled at this, observing, "Today, everything is done online so it's incredibly difficult." Never one to meekly adhere to a directive that he found objectionable, Schulte chose to ignore the condition. In December, the government presented evidence that he had defied court orders by going online, and on several occasions had even logged on to the Internet using Tor—a system that enables users to access Web sites anonymously. Meanwhile, authorities in Virginia charged him with sexual assault, citing as evidence the photograph discovered on his phone. Schulte was taken into custody once again and locked up at the Metropolitan Correctional Center, in Manhattan. He was still there in the summer of 2018, when the government filed a superseding indictment with ten new counts and charged him with leaking Vault 7.

"I finally meet my new celly," Schulte wrote, in a prison diary. "He's in for bankruptcy. He's a nice guy who is on medication for a mental illness." Schulte hated confinement

("If you try to shower without purchasing shower shoes then you will almost certainly contract MRSA or some other skin-eating staph bacteria"), but he appears to have found ways to keep his temper under control, having observed that it was necessary to exercise basic diplomacy, given that some members of his new cohort were convicted murderers. He was fascinated by the innovative ways that inmates gamed prison regulations, noticing that many people "claim to be Muslim or Jewish" because doing so entitled them to supposedly better food. And he made some friends on the floor where he was housed, including Omar Amanat, a Wharton-educated financier who was facing charges related to conspiracy to commit securities fraud, and Carlos Luna, a seasoned drug trafficker. Schulte reflected, "I've lost my job, health insurance, friends, my reputation, and an entire year of my life—and this is only the beginning." But he vowed to go down swinging and "bring this 'justice' system crumbling to its knees."

First, he would need a phone. At the prison, he could make calls on pay phones—but they were monitored and did not offer Internet access. Luckily, black-market smartphones were easy to come by: Luna had a sideline in smuggling them into the facility. According to a former inmate who did time at the M.C.C. alongside Schulte, the going rate there for a contraband smartphone was several thousand dollars. Schulte figured out a way to hot-wire a light switch in his cell so that it worked as a cell-phone charger. (The person who knew Schulte during this period praised his innovation, saying, "After that, all M.C.C. phones were charged that way.") Schulte and Amanat, who had also obtained a phone, would meet in the cell of a guy named Chino, and Luna would serve as lookout while the others used their clandestine devices. On an encrypted Samsung phone, Schulte created an anonymous Facebook page called John Galt's Legal Defense Fund and posted some of his prison writings. He set up a Twitter account, @FreeJasonBourne, and, in a drafts folder, he saved a tweet that said, "The @Department of Justice arrested the wrong man for Vault 7. I personally know exactly what happened, as do many others. Why are they covering it up?" Schulte also contacted Shane Harris, a journalist at the Washington *Post*. In messages to Harris, Schulte pretended to be other people—a cousin, or one of his three brothers—and promised to share explosive information. In this sock-puppet guise, he sent Harris what the government alleges was classified information about his case.

Astonishingly, it appears that Schulte may have even made contact with WikiLeaks during this period. In a Twitter post on June 19, 2018, WikiLeaks released seven installments of Schulte's prison writings, billing them as an account in which the "Alleged CIA #Vault7

whistleblower" would finally speak out in "his own words." Schulte seems to have envisaged these essays, which combined diaristic accounts of prison life with a broader critique of the criminal-justice system, as a sort of "Letter from a Birmingham Jail." He titled them "Presumption of Innocence." Perhaps WikiLeaks simply stumbled on the Facebook page where these essays appeared—or perhaps it was in touch with Schulte. If indeed Schulte managed to contact WikiLeaks from prison, he was adopting a curious strategy: it would be pathologically self-sabotaging to counter allegations that he had shared a set of documents with WikiLeaks by sharing another set of documents with WikiLeaks.

In one of these jailhouse meditations, Schulte wrote that, in prison, it is prudent not to discuss your case with anyone, because "people are vultures and will do anything to help their own situation"—including barter your information for a better deal. "Any scenario that encourages disloyalty, dissention, and 'snitching' is a powerful psychological tool," he warned. But Schulte may not have appreciated quite how true this was, because at a certain point his trusty lookout, Carlos Luna, informed prison authorities that Schulte had a cell phone.

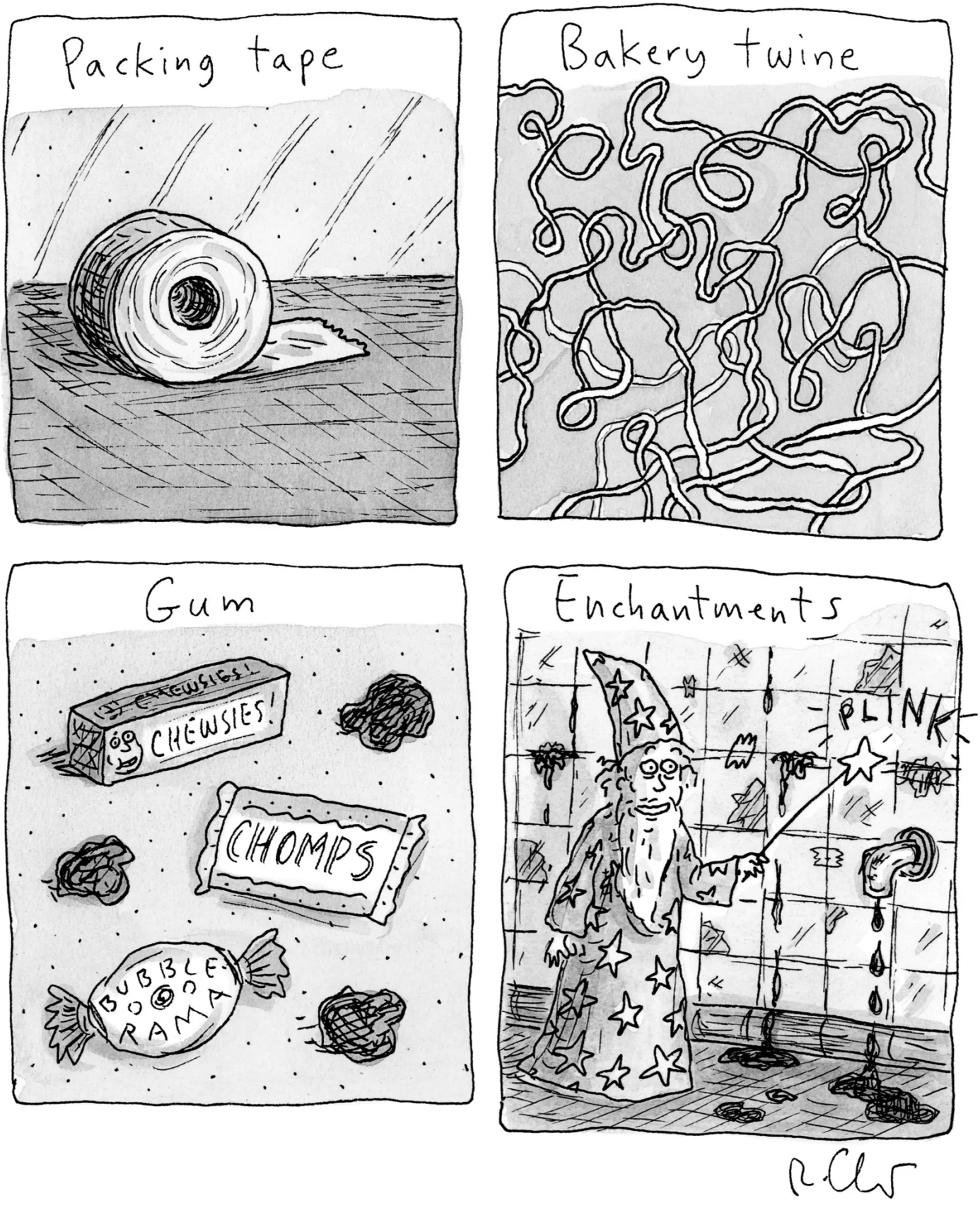
When this news reached the F.B.I., officials panicked: if Schulte could surreptitiously make calls and access the Internet, there was a danger that he was continuing to leak. "There was a great deal of urgency to find the phone," one Bureau official later acknowledged. One day in October, 2018, no fewer than fifty agents descended on the Metropolitan Correctional Center, accompanied by a cell-phone-sniffing dog. After they recovered the device, investigators found that it was encrypted—but also that Schulte, true to form, had written the password down in one of his notebooks. He was placed in solitary confinement.

The criminal trial of Joshua Schulte, which commenced on February 4, 2020, at the federal courthouse in Manhattan, was unlike any other in U.S. history. A decision had been made to postpone the child-pornography indictment and the Virginia sexual-assault charge; both cases could be pursued at a later date. For now, the government focussed on Vault 7, issuing ten charges, ranging from lying to the F.B.I. to illegal transmission of classified information. It had taken federal prosecutors three years to assemble the evidence that they would present in court, in part because of the official secrecy involved and in part because they intended to summon more than a dozen C.I.A. officers to testify, under oath, about Schulte's tenure at the O.S.B. This was a delicate and highly unusual strategy. To speak in public about what happens on the job is to violate one of the signature prohibitions

of an agency career. It was an indication of how seriously C.I.A. officials took Schulte's alleged offenses that they were prepared to forgo this traditional reticence for the purposes of a trial.

As the proceedings got under way, the theatre of secrecy was conspicuous: most of the C.I.A. witnesses would appear using pseudonyms, or would be identified only by their first names. (The agency declined to comment for this story, or to make any of the relevant officials available; much of this account is drawn from their trial testimony.) Agency witnesses further avoided scrutiny by using a special elevator; during their testimony, the courtroom was closed to the public. These precautions seemed somewhat excessive. After all, the witnesses were not covert operatives with assumed names, or highly placed U.S. assets in treacherous circumstances abroad. They were, by and large, just like Josh Schulte: E-ZPass warriors who lived in the D.C. suburbs and commuted to an office park. It was a stretch to suggest that the very fact of their employment at the C.I.A. amounted to a grand state secret.

WHAT HOLDS THE SUBWAY TOGETHER?



Cartoon by Roz Chast

One member of Schulte's defense team was Sabrina Shroff, a feisty and tenacious federal public defender who grew up in Islamabad. "You're going to have to take this as a given—I don't dwell on Mr. Schulte's shortcomings," she said, when I asked her about his volatility. "He's my client." We met at a coffee shop near Gramercy Park. Shroff is diminutive and intense, and quick to chuckle at the Kafkaesque predicaments of this case. But she was also severely constrained in what she could say to me. "We don't have the ability to cross-examine the classification authority," she pointed out; when the government designates something Secret, she cannot appeal the decision. Before the trial began, Shroff already possessed a Top Secret security clearance—she had needed one to defend other clients facing national-security charges—but in order to represent Schulte she had to be "read in" to even higher levels of fetishistically compartmentalized secrecy. All the classified material she would need to consult could be accessed only in a room on the ninth floor of the courthouse—a Sensitive Compartmented Information Facility, or SCIF, designed to house classified information. The defense team felt hamstrung in its efforts to represent its client. Normally, defense attorneys receive the names of prosecution witnesses in advance, and can research their backgrounds while preparing for cross-examination. When Shroff and her fellow-attorneys got the names, however, they were prohibited from performing any Google searches that might in any way link these individuals to the C.I.A. Because some witnesses had common names, and Shroff and her team could not add the letters "C.I.A." to their search terms, it was occasionally impossible to gather any information. "These are *shadows* to us," one of Shroff's partners, Edward Zas, protested to the judge in the case, Paul Crotty. "We are completely blind."

Every day of the trial, a small posse of blond women in professional garb arrived and sat together, observing. They kept to themselves and didn't speak to anyone else, but it was generally understood that they were lawyers or officials from the C.I.A. Their facial expressions uniformly unrevealing, they came and went in lockstep, like Stepford Wives, but they radiated muted power.

The parade of witnesses from the C.I.A. offered a rare glimpse of the office dynamics in a Top Secret unit. It was sobering. The descriptions of Schulte's workplace called to mind not the steely competence of "The Bourne Identity" but, rather, the tiresome high jinks and

petty scheming of "Office Space." This was the paradox of the proceedings: there was no way for the C.I.A. to exact retribution against Schulte without, in the process, revealing a great deal of unflattering information about itself. Jurors would be told the story of an élite national-security division that had become consumed by juvenile name-calling and recrimination; senior C.I.A. officials would have to submit to cross-examination about the frequency and the severity of Nerf-gun fights, or about the lax security that had made the breach possible. Schulte's former colleagues portrayed him as thin-skinned and volcanically malicious, and this proved to be the core of the government's case. "He's not some kind of whistle-blower," one of the prosecutors, David Denton, told the jury. "He did it out of spite. He did it because he was angry and disgruntled at work."

But Shroff's defense strategy rested on a sly pivot: she readily conceded that Schulte was an asshole. "He antagonized his colleagues," she said. "He antagonized management. He really was a difficult employee." Nevertheless, she added, "being a difficult employee does not make you a criminal."

Shroff further suggested that the story of Vault 7 was a parable not about the rash decision of one traitor but about the systemic ineptitude of the C.I.A. The agency didn't even realize that it had been robbed, she pointed out, until WikiLeaks began posting the disclosures. "For God's sakes," Shroff said in court. "They went a whole year without knowing that their super-secure system had been hacked." Then the agency embarked on a witch hunt, she continued, and quickly settled on an "easy target": Schulte. Within this narrative, the string of prosecution witnesses recounting horror stories about Schulte's workplace behavior almost seemed to play in Shroff's favor. Her client was a scapegoat, she insisted—the guy nobody liked.

The government had amassed a powerful case indicating that Schulte was the leaker. It was abundantly clear that he had motivations for taking revenge on the C.I.A. The professional biography that emerged at trial was so damning that a decision to leak terabytes of classified data seemed almost like a logical dénouement: the final explosion of a man whose nickname was literally the Nuclear Option. Schulte's incriminating Google searches further deepened his appearance of guilt. And, on the sixth day of the trial, prosecutors laid out what they regarded as a coup de grâce—the digital equivalent of fingerprints at a crime scene. Even after Schulte was stripped of his administrative privileges, he had secretly retained the ability to access the O.S.B. network through a back

door, by using a special key that he had set up. The password was KingJosh3000. The government contended that on April 20, 2016, Schulte had used his key to enter the system. The files were backed up every day, and while he was logged on Schulte accessed one particular backup—not from that day but from six weeks earlier, on March 3rd. The O.S.B. files released by WikiLeaks were identical to the backup from March 3, 2016. As Denton told the jurors, it was the "exact backup, the exact secrets, put out by WikiLeaks."

But all this was quite a complex fact pattern to present to a jury, involving virtual machines and administrative privileges and backups and logs; much of the expert testimony presented by the prosecutors was bewilderingly technical. Shroff, meanwhile, insisted that Schulte hadn't stolen the data. Perhaps someone else in the office—or at the agency—had done it. The real outrage was that a crucial C.I.A. computer network, DevLAN, had been unprotected. Hundreds of people had access to DevLAN, including not just C.I.A. employees but contractors. The C.I.A.'s hackers appear to have disregarded even the kinds of elementary information-security protocols that any civilian worker bee can recite from mandatory corporate training. Coders exchanged passwords with one another, and sometimes shared sensitive details on Post-it notes. They used passwords that were laughably weak, including 123ABCdef. (A classified damage assessment conducted by the C.I.A. after the Vault 7 exposure concluded that security procedures had indeed been "woefully lax," and that the agency's hackers "prioritized building cyber weapons at the expense of securing their own systems.")

Nevertheless, the prosecutors presented striking circumstantial evidence indicating that Schulte had probably transmitted the material to WikiLeaks. On April 24th, he downloaded Tails, an operating system that WikiLeaks recommends for submitting data to the organization; on April 30th, he stayed up all night, frequently checking his computer, and at 3:21 A.M. he consulted a Web page that offered guidance on how to make sure that a terabyte of data has been "transferred correctly." That evening, he also searched for tips on how to wipe a device of its contents. What the government could not prove was any direct communication between Schulte and WikiLeaks.

Hovering over the proceedings was a dark question: how much harm had been caused by the leak? When Shroff cross-examined Sean Roche, the C.I.A. official who described Vault 7 as a "digital Pearl Harbor," she asked, "How many people died in Pearl Harbor?"

“More than three thousand,” Roche replied.

How many people died as a result of Vault 7? she asked.

“I don’t have an answer to that,” Roche said.

“Can you try to get my plants on the fire escape?”

Cartoon by Jon Adams

“In fact, none, correct?” Shroff said.

Roche was probably being hyperbolic. But this may have been an instance in which the secrecy surrounding the case put the *government* at a disadvantage. After China uncovered a network of U.S. intelligence assets operating inside its borders in 2010, authorities in Beijing systematically rounded up a dozen people who had secretly been working for the C.I.A. and murdered them, crippling American espionage efforts in the country for years to come. That deadly purge did not become public knowledge until it was reported in the press, in 2017. Given that the O.S.B. hacks often required human assistance to install, it seems possible that foreign powers penetrated by such exploits could have leveraged the leak to identify American assets and seek retribution in a manner similar to what occurred in China. If any countries did—or if they do so in the future—that is information that the C.I.A. would be unlikely to publicize.

One morning in March, 2020, the jurors in the Schulte case entered the courtroom to discover a giant bottle of Purell on a table. The attorneys had been so consumed by the case that they had hardly noticed the pandemic barrelling toward them. Meanwhile, one of the jurors ended up being removed from the case, because, much like Schulte himself, she couldn't stay off the Internet. (The normal prohibition on jurors reading press coverage was particularly acute in this instance, because, if the jury knew that Schulte had also been charged with sexual assault and possession of child pornography, it could prejudice the verdict.) The juror seemed only too happy to be cut loose, telling the *Post*, "Sitting in that chair for five weeks was like punishment for my ass." After Shroff delivered an emphatic closing argument in the case, she visited the bathroom, where she crossed paths with one of the Stepford Wives. Up to this point, none of these C.I.A. women had uttered a word to her. "Nice job," the woman said, crisply, and walked out.

As the jurors began deliberations, they sent out a series of notes with questions that seemed to indicate some genuine confusion about the technical aspects of the government's case. On March 9th, they convicted Schulte of two lesser charges—contempt of court and lying to the F.B.I.—but hung on the eight more serious counts, including those accusing him of transmitting national-security secrets to WikiLeaks. Judge Crotty declared a mistrial.

The prosecution had clearly blundered by getting so mired in technical minutiae, and Shroff had ably defended her client. But it was also tempting to wonder whether in the years since WikiLeaks was established, in 2006, public attitudes toward both the intelligence community and the act of leaking itself might have shifted. Endless revelations

concerning warrantless wiretapping, the use of torture, and extrajudicial killing have done little to enhance the prestige or the moral standing of America's defense and intelligence establishment. And many people consider Snowden and Manning, along with Julian Assange, the founder of WikiLeaks, to be heroes. Of course, in Schulte's case there did not appear to be any moral imperative driving the leak. If he did it, he wasn't blowing the whistle but seeking payback. And he continued to deny that he did it. Edward Lee Howard, the disgruntled C.I.A. officer who handed secrets to the Soviets, went to his death denying that he had done so. The person who served time with Schulte in the M.C.C. said, "What Josh told me is that he thinks Amol set him up."

The mistrial was a devastating turn for the government, but Schulte's father, who came from Texas with Deanna to attend the proceedings and staunchly believed in his innocence, was disappointed. Roger Schulte, who didn't know what a hung jury was, asked Shroff, "You mean he wasn't acquitted?" The child-pornography and sexual-assault cases have still not been resolved. When I asked Roger and Deanna about those charges, they said that, though they believe in Josh's innocence, they haven't spoken to him about the particulars of either case, or examined the available evidence themselves, so they were not in a position to offer any preview of his defense. But the U.S. government, rather than push forward with these other cases—which might have resulted in an easier conviction—instead announced that it would put Schulte on trial again for Vault 7.

Schulte currently resides at the Metropolitan Detention Center, in Brooklyn, where he has been preparing for his new trial. Most observers of the case agree that Schulte is fortunate to have a lawyer like Shroff, but he doesn't necessarily share this view; after the government announced that it would retry him, he dismissed her and opted to represent himself. Shroff has stayed on, however, as standby counsel. "I've been with Mr. Schulte for five years," she said. "We went through a pandemic together, we went through a trial together—most marriages don't survive this kind of trauma." Shroff told me that she and Schulte spend hours on end in the SCIF, where he is formulating his new defense, along with another lawyer, Deborah Colson, and a paralegal. For security reasons, they can't take garbage out of the room, so trash accumulates among the boxes of highly classified documents. The lawyers used to bring Schulte snacks (gummy bears, Dr Pepper) before the Marshals banned food in the SCIF. "He's such a persnickety eater," Shroff said, with

affectionate exasperation. “If I go to Chipotle, it has to be white rice and only black beans.” In prison, Schulte has grown an impressive beard.

To nobody’s surprise, Schulte has tangled with his prison guards, and in repeated filings to the new judge in his case, Jesse M. Furman, he has singled out individual guards and suggested that *they* should be facing criminal charges. Schulte has filed more than sixty official challenges to the conditions of his confinement. In prolix memos, many of them handwritten, he has condemned the Justice Department, the C.I.A., the F.B.I., and the Bureau of Prisons. He refers to his cell as a “torture cage,” and maintains that his living conditions are “below that of impoverished persons living in third world countries.” One of his complaints is that the guards do not give him adequate bathroom breaks during the hours he spends preparing his case in the prison law library. And so, lately, Schulte has taken to urinating in the law library. He has also converted to Islam. When I mentioned this to Kavi Patel, he burst out laughing. “He’s manipulative,” Patel said. “I don’t know how else to say it.” One might question whether this conversion is simply a ploy to get better food. But many people discover faith behind bars, and Schulte recently observed a month of daytime fasting during Ramadan.

The new trial is scheduled to begin on June 13th. The government seems unlikely to present quite as much evidence of Schulte’s antisocial behavior this time. It may abbreviate the technical evidence, too. The proceedings, however, will remain blanketed in secrecy: Matthew Russell Lee, an independent journalist who covered the first trial, recently filed an objection to the government’s motion to seal the courtroom during testimony from C.I.A. officers, but it appears that that condition will again apply. Schulte, meanwhile, has sought to call no fewer than forty-eight current or former C.I.A. employees as witnesses. One of the people he has tried to summon is Amol. At a recent hearing, Schulte suggested that, if the evidence he requests is too sensitive to transport to the SCIF, perhaps “they should take *me* to the C.I.A.” Judge Furman responded flatly, “You are not going to the C.I.A.”

We live in an era that has been profoundly warped by the headstrong impulses of men who are technically sophisticated but emotionally immature. From the whoopie-cushion antics of Elon Musk to the Panglossian implacability of Mark Zuckerberg, a particular personality profile dominates these times: the boy emperor. While reporting this article, I often wondered how the C.I.A. could have missed the obvious combustibility of this profile when it hired Schulte and gave him a security clearance. In order to get an

agency job, Schulte had been subjected to a battery of tests—but, when his lawyers tried to obtain the psychological profile that the agency had produced on him, the C.I.A. would not turn it over. Perhaps, as the agency took up digital spying and sought to bolster its hacking capability, it deëmphasized qualities like emotional stability and sang-froid, and turned a blind eye to the sorts of erratic or antisocial tendencies that are widely accepted in Silicon Valley (and even embraced as the price of genius). The agency may have been blinkered about Schulte's destructive potential because it had concluded that this was simply how coders behave. I sometimes found myself wondering whether Schulte was more idiot or savant.

When you consider the powerful forces arrayed against him—and the balance of probabilities that he is guilty—Schulte's decision to represent himself seems reckless. But, for the C.I.A. and the Justice Department, he remains a formidable adversary, because he is bent on destroying them, he has little to lose, and his head is full of classified information. "Lawyers are bound," Shroff told me. "There are certain things we can't argue, certain arguments we can't make. But if you're *pro se*"—representing yourself—"you can make all the motions you want. You can really try your case."

The government does not bring a lawsuit every time it identifies somebody who has inappropriately leaked classified information. On the contrary, a decision is often made to settle the matter quietly, rather than risk further exposure of secrets in a public trial. Schulte might well attempt to force the disclosure of so many secrets that the authorities will feel compelled to drop the charges against him or to offer an attractive plea deal. There may be some threshold of disclosure beyond which the C.I.A. will not venture. Deanna Schulte told me that one reason her son had elected to serve as his own counsel is that he wants to "put it all out there."

In a June 2nd court filing, Schulte suggested, with a menacing flourish, that if the government goes to trial with the child-pornography charges he plans to make it maximally painful for the C.I.A. His defense, he promised, will incorporate extensive testimony about agency "operations and assets," and will potentially require courtroom appearances from "9 covert officers, 17 overt officers, and at least 1 asset."

In a contest between the dictates of official secrecy and the imperatives of justice, odds are that secrecy will win. Schulte knows this, and that may be his greatest advantage. He has

said of the Vault 7 case, “I expect a not guilty verdict on all counts, and anything less will be an utter failure.” Shroff told me of her client, “He’s hopeful now.” Roger Schulte said the same thing, assuring me that Josh has learned a lot about the legal process, and that he isn’t giving up. “He seems to be holding pretty strong,” Roger said. “He’s a fighter.” ♦

Published in the print edition of the June 13, 2022, issue, with the headline “King Josh.”

NEW YORKER FAVORITES

- The attorney fighting revenge porn.
- Pauli Murray was an architect of the civil-rights struggle—and the women’s movement. Why haven’t you heard of her?
- What old money looks like in America, and who pays for it.
- An MSG convert visits the high church of Umami.
- Why the archives of so many great writers end up in Texas.
- Fiction by Donna Tartt: “Tam-O’-Shanter”

Sign up for our daily newsletter to receive the best stories from *The New Yorker*.

Patrick Radden Keefe, a staff writer at The New Yorker, is the author of “Empire of Pain.” His new book is “Rogues: True Stories of Grifters, Killers, Rebels, and Crooks.”

More: Central Intelligence Agency Hackers Code Data WikiLeaks Intelligence Secrecy

THE NEW YORKER CLASSICS

Classic pieces and hidden gems curated by our archive editor, Erin Overbey, and delivered twice weekly.

E-mail address

Your e-mail address

Sign up

By signing up, you agree to our User Agreement and Privacy Policy & Cookie Statement.