

HARPER'S

M A G A Z I N E

April 15, 2017: [[Afghanistan](#)][[Planned Parenthood](#)][[Amnesty International](#)][[Saturn \(Planet\)](#)]

[ARCHIVE](#) / [2017](#) / [May](#)

[< Previous Article](#) | [Next Article >](#)

[Report](#) — From the May 2017 issue

Snowden's Box

The human network behind the biggest leak of all

By [Jessica Bruder](#), [Dale Maharidge](#)

[Download Pdf](#)

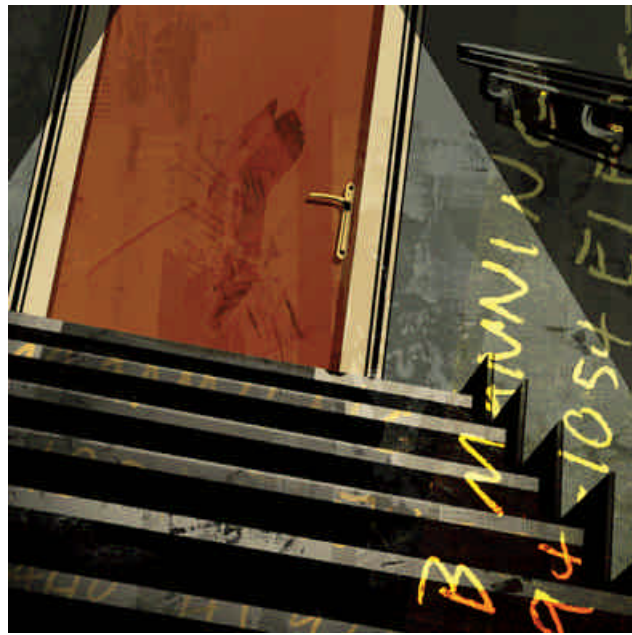
[Read Online](#)

[Single Page](#)

[Print Page](#)

MAHARIDGE

It was a frigid winter, and the Manhattan loft was cold — very cold. Something was wrong with the gas line and there was no heat. In a corner, surrounding the bed, sheets had been hung from cords to form a de facto tent with a small electric heater running inside. But the oddities didn't end there: when I talked to the woman who lived in the loft about her work, she made me take the battery out of my cell phone and stash the device in her refrigerator. People who have dated in New York City for any length of time believe that they've seen everything — this was something new.



That I was in her loft in the first place was strange enough. A year earlier, I was supposed to get married, but the engagement fell apart. After that, I was in no shape for a relationship, and was in any case finishing two books on tight deadlines. I should have been too busy, then, to go to a party in Park Slope, Brooklyn, on a December evening in 2011. The host, Julian Rubinstein, had invited a group of his friends, many of whom were writers, musicians, editors, and documentary-film makers. His email billed the event as a “fireside gathering,” although when he attempted to get a blaze going in the hearth, the apartment filled with smoke. Through the haze, I noticed a striking woman with dark hair occasionally glancing my way.

“Who’s that?” I asked Julian.

Illustrations by Taylor Callery

He introduced me to Laura Poitras. I was aware of her 2006 documentary, *My Country, My Country*, about an Iraqi physician running for

office in his country’s first democratic election. Her current project, she told me, involved filming the massive data center the National Security Agency was building in Utah. Our conversation was intense, and I found myself wondering why somebody as sophisticated as Laura would be interested in me — at heart, I still felt like a blue-collar kid from Cleveland.

Suddenly, she announced it was late. “Want to share a cab?” she asked.

I shambled down two flights of stairs after Laura, and we hailed a taxi. We shook hands when we reached her stop and I continued north. Two nights later, we met for drinks, and exchanged a lot of passionate talk — about our work. When I saw her name in my email inbox the next morning, I clicked eagerly. Maybe she wanted to go out again? She briefly raised that as a possibility, but Laura had something more important in mind. Her message read:

If you want to set up a secure way to communicate (which I think every journalist should) the best method is IM with an OTR encryption. You’ll need: a Jabber account, Pidgin IM client, and OTR plug-in.

Five years ago, this request — which would now strike many journalists as completely reasonable — sounded like gibberish. Why did I need encryption? I’d never done a story that would interest the NSA or any other federal agency. I initially blew off her advice, even as we got involved and began opening up about our projects. Which is how I came to be in that freezing loft, where Laura patiently explained why it made sense for me to put my phone in the fridge. I hadn’t known that a refrigerator could block cellular signals. For that matter, I hadn’t known that even when a cell phone is switched off, the NSA can still use it to eavesdrop on conversations.

Hers, I soon realized, was anything but idle paranoia. Laura had been interrogated by U.S. Customs and Border Patrol agents on more than forty occasions when traveling internationally. Sometimes they temporarily confiscated her notebooks. Once, they took away her computer. On April 6, 2012, after we had known each other for about four months, Laura was grilled at Newark Liberty International Airport when she was coming home from London. As always, following her lawyer’s instructions, she took notes. This time, a federal agent declared that her pen was a potential weapon and threatened to handcuff her. I was on a reporting trip in the rust belt, en route home from the Monongahela Valley, and expressed my concern in an email. “It was actually quite humorous,” she replied, “if it weren’t so outrageous.”¹

¹ On this occasion, Laura reached out to the journalist Glenn Greenwald, who

In early August, Laura visited the solar-powered off-the-grid home I’d built in northern California, overlooking the Pacific. The place is very remote, with the nearest utility lines some three miles away and the closest neighbor a half mile (as the spotted owl flies) across a canyon. There she edited *The Program*, a short documentary for the *New York Times* about the NSA’s collection of personal data, featuring the whistleblower William Binney. She returned to New York to resume work on a larger project, and ultimately decided that she needed a more secure location to edit it. A few weeks later, she found one: Berlin.

Meanwhile, she was contracting out a major renovation of her New York loft. Having been a professional chef in the Bay Area before she made her first film, *Flag Wars*, she was especially eager to have a working kitchen. Because I'd remodeled and built homes, she asked for advice. I offered suggestions on such things as countertop materials (she chose concrete).

We remained involved, albeit with an ocean between us. She briefly visited New York in October. I tried (and failed) to fix a leaking bathroom pipe in her apartment, which was still without heat. That aside, I didn't see her for the rest of the year. We emailed — she answered promptly no matter what time of the day or night I wrote her. I knew some of what was going on in her life, but not everything. There was, for example, the note she made in her diary on January 17, 2013:

² *Excerpts from Laura's diary, "Berlin Journal," first appeared in Astro Nois*

Just received email from a potential source in the intelligence community. Is it a trap, is he crazy, or is this something real?²

Little more than a week after making that diary entry, Laura returned to the United States to shoot footage of the NSA's Utah Data Center, which was still under construction. According to the journalist James Bamford, the facility, which would begin operations in 2014, was designed as a repository for

all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails — parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter."

With these matters on her mind, Laura flew back to New York, where she told me about getting approached by the mysterious source. "Could it be a setup?" she asked. It could. Yet she chose to keep the channel open. We adopted a code for talking about the issue, pretending that we were discussing the ongoing renovation of her loft. On the last day of January, I invited Laura to dinner at my place, and she replied, "I had a really good meeting with the contractor today. I look forward to updating you." That meant she had communicated with the source.

We talked about the source over dinner, and Laura told me that this person wanted a physical address to use in case (as the source put it) "something happens to you or me." We speculated that perhaps this person might want to send her a parcel. Hard copy? Data? It was unclear. Needless to say, the material couldn't go directly to Laura: her mail was surely being scrutinized. Nor could I receive it, because of our connection. She said we needed a third party, someone who wouldn't be on the NSA's radar.

"Do you know someone, a journalist, whom you absolutely trust?" she said. "Someone who won't ask any questions?"

"Sure," I responded. I immediately thought of the perfect person. She had just moved, and I didn't have her new address, but I told Laura that I would supply the contact information soon. The next time we met, I gave Laura the address, and then we spent some time refining our code to use on the phone and in emails, since she was going back to Berlin. (Incredible as it now sounds, I had not yet begun using encryption.) We would call the unnamed source the "architect" and refer to the mysterious shipment as "architectural materials." The recipient of the package would be called the "sink." Should that person prove to be unavailable, I would find a backup choice, whom we would call the "other sink." The NSA or FBI would be called the "co-op board" — a tribute to the truculent nature

of such boards in New York City. And if either of us wrote, “The carpenter quit the job,” that meant it was time to start over with a new plan.

Hours later, Laura emailed from the airport: “Thanks for checking in on the renovation work while I’m away. Hopefully it will be drama free, but that might be wishful thinking.” I wrote her back on February 12: “That first sink is definitely the cool one. You always want to go with stainless steel. I hate porcelain.”

BRUDER

Over the course of nearly a decade and a half of friendship, Dale and I have shared all sorts of experiences. We have accidentally driven over a cow after midnight on the high plains of Colorado. We have extracted a rancher pinned against a tree by his pickup, and pruned branches from some of the taller trees on Dale’s California property using a shotgun. (They had been blocking his ocean view.) We often jokingly refer to ourselves as a platonic married couple. I was confident that there was nothing he couldn’t tell me. I was wrong.

In February 2013, I was hanging out at Dale’s apartment near the Columbia Journalism School, preparing to teach a class. He made an offhand request: would I be willing to receive a package in the mail for one of his friends? He didn’t say whom the package was for or what it would contain. He just blurted something vague about “investigative journalism.” I wouldn’t be able to ask any questions, he added. Could I handle that?

“Sure,” I said. “No problem.”

The package, he continued, would be labeled ARCHITECTURAL MATERIALS ENCLOSED. I should not open it. And we would never, ever speak about it over the phone. Any mention of the shipment had to be in code.

“We’ll call it the ‘elk antlers,’ ” Dale said soberly. This was a reference to my dog’s favorite treats, which arrived regularly at my apartment by mail.



I tried to keep a straight face. “So when it comes, I’ll tell you, ‘I’ve got the elk antlers.’ ”

“Exactly.”

This sounds like a bad spy movie, I thought. But how do you tell that to someone you ran over a cow with? In any case, for more than three months after Dale made his request, nothing happened. As I would later learn, he and Laura were exchanging constant updates, with occasional confusion as to whether they were discussing her mystery source or the actual renovation, which was still going on.³ Before long I had forgotten about the whole thing, busy with my own writing and teaching.

³ On March 15, for example, Laura emailed

Then, on May 14, I returned home to Brooklyn after finishing an assignment in Los Angeles. I climbed the stairs to the fourth-floor landing. In front of my door was a box.

That was weird. No one ever bothered to walk all the way up to the fourth floor. Packages usually arrived in a haphazard scatter in the lobby. Sometimes they didn't stick around for long — in recent months, quite a few boxes had disappeared in a spate of thefts. Their contents included vitamins, an LED tent lantern, a pair of earbuds, Magic Grow sponge-capsule safari animals, and a copy of Evgeny Morozov's *To Save Everything, Click Here*. My bicycle, too, had been stolen from the boiler room in the basement. But the thieves had turned up their noses at this latest package.



I picked up the box. The words ARCHITECT MATS ENCL'D were scrawled in block letters on the front. How long has this been sitting here? I wondered. After letting myself into the apartment, I took a closer look. Nothing about the package appeared unusual at first. It had been postmarked May 10 in Kunia, Hawaii, and sent via USPS Priority Mail. I shook the box gently, like a child guessing at the contents of a gift. Something inside made a clunking noise. Otherwise it gave up no secrets.

Then I noticed the return address:

B MANNING

94-1054 ELEU ST

WAIPAHU, HI 96797

What the fuck? I thought. Is this a joke? There was no way this package had come from the Army intelligence specialist turned Wikileaker. At the time, Bradley (now Chelsea) Manning was in military prison, awaiting a court-martial. A few hours later, after calling Dale to let him know that the elk antlers had arrived, I tucked the box into a messenger bag and drove into Manhattan. When I arrived at Dale's apartment, I thrust the box into his hand.

"Check this out!" I gestured at the return address. "Your friend sure has a puckish sense of humor."

Dale looked equally confused. Soon we gave up puzzling over it and went out to dinner.

MAHARIDGE

The rest of May wasn't measured in minutes, hours, or even days — rather, it was marked by steadily increasing levels of anxiety. The calendar says it was two weeks, but for me, it was a single, excruciating unit of time. And if this was how I felt, what was Laura dealing with? As I would later learn, she had copied a quote from George Orwell's *1984* into her diary: "Your worst enemy, he reflected, was your own nervous system. At any moment the tension inside you was liable to translate itself into some visible symptom."

Laura arrived back in the United States on May 15. It was late at night, but she came straight to my apartment from the airport to get the box. Instead of opening it, she booked a hotel using my

computer, then sped off in a taxi around two in the morning. For the next few days, she communicated with her source — who remained anonymous — from the hotel. The box contained data and instructions, and there was a growing sense that it involved something momentous. The source, Laura said, was treating the matter “a bit like a puzzle.” There were multiple layers protecting the data, little of which she had seen. Meanwhile, she was slowly convincing the source to meet with her, while trying to gauge whether this person was trustworthy in the first place.

To lessen the tension, we turned to gallows humor. One night, Laura and I met up with her friend Kirsten Johnson for drinks and dinner. “When you get sent to Guantánamo, Dale and I will take turns using your steam shower,” Kirsten said, alluding to Laura’s renovation. But we knew it was serious business, and now Laura insisted that I begin communicating with her in a more secure manner.

She set me up with The Amnesic Incognito Live System (Tails), a high-end encryption program that funnels all internet traffic through the anonymous Tor network. Tails uses a USB flash drive, bypassing the computer’s operating system. All I had to do was plug in the drive that Laura gave me, turn on the computer, and wait for the connection to be routed through proxy servers. There was a tiny yellow onion in the upper-right-hand corner of the screen — a homage to Tor’s original name, The Onion Router — and when it turned green, it was safe to communicate.

For the next two weeks, Laura and I were in constant contact. The source, who still hadn’t given her a name, now suggested that they meet. This was tempting, but it also raised the stakes considerably, and we spent much time speculating: was the source affiliated with the CIA or the NSA? He or she seemed to span agencies, Laura said. But that was just a suspicion on her part.

I was feeling in over my head. I’m more of a narrative or cultural journalist. I had been in my share of hairy situations when covering conflict overseas, or even here in the United States. This, however, was a new dimension. I feigned steadiness when offering Laura advice, but my stomach was constantly churning.

One night, when Tails refused to work on my computer, Laura fell back on email. At 4:49 A.M., she wrote: “Can you get in a taxi? I really need to talk.” I ran downstairs and flagged a cab; as the vehicle sped down Broadway, I peered out the rear window to make sure I wasn’t being followed. When I arrived at her hotel room, Laura didn’t speak. She pointed to my phone: the battery came out and the device went in the fridge. Then, eyes wide, she pointed to a file on the computer screen. It was NSA data — part of an extensive trove of documents. “It looks like the entire U.S. government intelligence budget,” she said. Then she showed me a long message that was literary, even poetic. It was signed Edward Joseph Snowden.

She had only recently learned his name. She had also learned that she was more vulnerable than ever. Snowden warned Laura about what he called a “single point of failure.” At the moment, she was the only person who had the material, and if the federal government could stop its release, he said, they would take whatever steps necessary to do so. That had a bad sound to it, I thought, as I pondered the stunning scope of the story and the dangers it posed to Laura in particular. To remedy the situation, Snowden had urged her to get copies of what had come in the box into the hands of others.⁴

⁴ *Distributing leaked documents widely to avoid a single point of failure is*

Snowden, she said, had made it clear that he was no ordinary bureaucrat. Indeed, he insisted that

this leak was bigger than the Pentagon Papers. Nothing in my career as a journalist had prepared me for this moment, and quite understandably, Laura was also feeling overwhelmed. At one point she exclaimed, "I'm just a chef!"

Laura asked me to be one of the keepers of the material. My profile as a journalist and a professor at an Ivy League school, she felt, would afford some protection. "Would you do that?"

"Sure."

She warned of the possibility of grave risk. She wanted to be certain I understood the danger, that I knew I could say no. "This is what we do," I responded. "It's why we're journalists."

She muttered something about that being one of the reasons why she liked me. We embraced. The next night, a Thursday, we got together again. On Saturday, she flew to Hong Kong.

BRUDER

In the days after I passed the box to Dale, he intimated that he'd been learning more about it, but told me nothing. "Watch the news," he said. "You'll know when the story hits."

On June 5, the *Guardian* published a top-secret court ruling in which the U.S. government had ordered Verizon to turn over millions of customers' phone records "on an ongoing, daily basis." The newspaper was vague about the source of this classified information.

After reading the story, I called Dale: "Is that it?"

"Yes."

"Shit." I felt light-headed. "Is that all of it?"

"No."

Over the next few days, more disclosures followed. The NSA had been collecting users' private communications from AOL, Apple, Facebook, Google, Microsoft, Yahoo, and other companies. President Obama had told intelligence officials to make a list of possible foreign targets for American cyberattacks. During a single thirty-day period, the NSA had harvested nearly 3 billion pieces of intelligence from U.S. computer networks. And so on. Dale and I spoke again.

"All that stuff was in the box?"

"Yes."

"There must have been other boxes?"

"No."

The more details that emerged about the reach and sophistication of government surveillance, the more absurd our situation seemed. Some of the most sensitive intelligence information in the world had traveled in plain sight through the U.S. mail, then sat in my hallway, where it could have been pilfered as casually as all those other packages.

Thinking about that made my head spin. It also reflected what I consider to be one of the great lessons of adulthood: that most of the institutions and endeavors we regard as ironclad — from parenting to politics — are actually held together with chewing gum and duct tape. Nothing truly *works*, at least not for long, or not in the way it's supposed to. This reality is terrifying, because it exposes the precariousness of the existing order. But it's also liberating, because it encourages the individual to act, to defy the ominous mythology of competence and control.

The only person I could talk to about all this was Dale. But he didn't seem to know the full extent of what was happening either.

So now what? There was no way to predict how many more stories were coming or what they might reveal. I'd never been so close to something I knew so little about. It was bewildering, like having a front-row seat to a play performed in a language I didn't understand. Would I return home one day to find federal agents at my door? Should Dale and I be taking steps to protect ourselves?

Inaction was making me crazy. I needed to do something. On the roof above my apartment, I had built a picnic table out of blue wooden sawhorses, the kind the N.Y.P.D. uses for crowd control. Earlier I'd thought it was funny, a piece of antiauthoritarian patio furniture. Now it seemed like a liability — too visible — so I decided to cover it up. After that I felt a little better. But not much.

MAHARIDGE

I flew to Sacramento the same day that Laura traveled to Hong Kong. That last night we met, I worried about going to California with a copy of the material.

"Should I check it in a bag or take it as carry-on?"

"Carry it," Laura said. She gave me a withering look: to her, it was a silly question.

"What about security?"

"They won't notice it."

"Do you think they know?"

"If they knew, none of this would be happening."

I still worried about being busted. As I flew across the continent, with a copy of everything Snowden had sent us in an overhead bin, I wanted to get home to my off-grid place and stash the item as fast as possible.

As luck would have it, I got bogged down in Sacramento, because a crown came off during my flight and I had to wait several days to see my dentist. On June 6, meanwhile, the *Washington Post* broke its first Snowden story, which made me extremely anxious. Yet I still couldn't head up north, because a man named Shane Miller had shot and killed his wife and two daughters, ages eight and five, then abandoned his truck on the beach road right below my house. Miller, who had spent much time in those coastal woods, was believed to be holed up somewhere in the canyons and ridges surrounding my property. A manhunt was on. So I delayed my return by a few more days, until I couldn't take it anymore — I needed to hide the material *now*.

On Interstate 5, I noticed a blue truck right behind me; it remained at the same distance whether I

sped up or slowed down. I turned off on California 20. The truck disappeared. I stopped for coffee. Miles later, the blue truck was once again behind me, and then it was lost from sight, and then it reappeared on U.S. 101 before vanishing for good. Jesus! I flashed back to 1984, when I had been documenting the religious underground that brought Salvadoran refugees north from the country's civil war. For various reasons, I ended up smuggling a family with a toddler through northern Mexico, driving them in a panel wagon around a Mexican government checkpoint on dirt roads that vanished when we hit the base of the Sierra Madre, then heading north over rough terrain between the cacti and other desert flora.

I digress for a purpose. In El Salvador, government agents followed us openly. Ditto for Mexico. They wanted us to know we were being watched: it was a form of intimidation. Was this a similar tactic? Or was I simply being paranoid? In any case, the morning after I arrived home, a black helicopter was hovering over my land. Was it local cops looking for Miller, or the feds watching me? The previous night, I had sealed the Snowden material and placed it beneath the former outhouse, abandoned since I'd installed a septic system, inside a fifty-five-gallon barrel of old shit. It seemed way too obvious a hiding place. Eventually, the material ended eighty feet up an old-growth Douglas fir in my forest.

Through Laura, Snowden had instructed me to burn the original shipping box. She asked me to take video of the conflagration. I prepared to follow her instructions, but something stopped me — I couldn't bring myself to set the thing on fire.

I spent the next two weeks barricaded in my house with the shutters drawn. I had a loaded shotgun at the ready for Miller, but I was afraid of going outside with the weapon: that could be a fatal move if the feds showed up for the Snowden material. Eventually, though, I had to emerge to split log rounds for the woodstove, the building's sole source of heat. It was a Hobson's choice. When I went to the woodpile, I carried the gun.

BRUDER

For the rest of the month, disclosures from the Snowden archive continued. Life in Brooklyn was quiet, though. My worries began to abate.

Then July brought a new and startling revelation. The U.S. Postal Service had been photographing and logging every single piece of mail it processed: 160 billion items in 2012 alone. The practice was exposed by the *New York Times*, which declared that "postal mail is subject to the same kind of scrutiny that the National Security Agency has given to telephone calls and e-mail."

For a while it had seemed like good old-fashioned mail was one of the final frontiers of privacy — an analog holdout in a world where digital communications were increasingly insecure. Now it was clear that the system had limitations. Still, if used judiciously, it remained one of the safer ways to send data. Several months after the *Times* scoop, Jimmy Carter noted that he used snail mail as a sort of low-tech countersurveillance measure. "When I want to communicate with a foreign leader privately," he told *Meet the Press*, "I type or write a letter myself, put it in the post office, and mail it."

At some point after the box arrived and I made the handoff, Dale had recapped the original smuggling plan to me: Snowden was to pass the package along to someone else, who would in turn mail it to me. Then I would bring the package to Dale, who would give it to Laura. The idea was to ensure safety by insulating both ends of the transaction. Neither the sender of the package nor its final recipient would be involved with the shipping process, where the information was most

vulnerable.

But something was off. I went to my laptop to consult a photograph of the box I'd taken before delivering it to Dale. I reviewed the return address again:

B MANNING

94-1054 ELEU ST

WAIPAHU, HI 96797

Shortly after Snowden unmasked himself, the media had descended on Waipahu, where he had rented a home about seven miles south of the NSA's Kunia Regional Security Operations Center, his former workplace. In one of the news reports I found out that he lived at 94-1044 Eleu Street. Snowden, it would appear, had addressed the package himself. And he had done it while flipping the bird to the U.S. Postal Service: using the pseudonym B. Manning, changing only a single digit of his address.

This amazed me. Why bother taking precautions if you're going to play a joke like that? What's more, he had written my full name and address on the box: information I had volunteered because I trusted Dale. Now anyone who wanted to track packages sent from Waipahu to New York in the month of May — how many could there have been, really? — would easily identify the shipment. Someday, I vowed, I'd ask Snowden why he had done that. Why not ship the box under a random name, from some other town? For now, I just hoped it wouldn't jeopardize the security of the operation or get me burned.

There was something else on the box I hadn't noticed before: a bar code with a tracking number. I was very tempted to plug it into the USPS website and find out how long the package had sat in my hallway. But I was already nervous and decided against that.⁵

⁵ *A good choice, as it turns out. The USPS logs the IP addresses of all custo*

In fact, the whole situation was making me uneasy. Snowden had fled from Hong Kong to Moscow, where he was seeking asylum. Glenn Greenwald was in Rio de Janeiro, where he lived. Laura had decamped once again to Berlin.

The next time I spoke to Dale, I had a new question.

"Are we the only people who had anything to do with this who haven't left the country?"

"I don't know," he said.

Perhaps there were others, we decided: additional bit players in the affair, living in separate silos of paranoia. There was no way to tell.

THE PLAYERS

In 2013, we had started referring to Laura as the Chef, because of her previous career. Three years later, we learned that title was apt in another way. As the Snowden story unfolded, she had masterfully orchestrated the various players required to transmit and safeguard his information, as if

working with ingredients in a recipe.

As far as we know, there were five of us. In other words, three other volunteers had received duplicates of Snowden's shipment before Laura traveled to Hong Kong. He had viewed his meeting with Laura as extremely risky, she told us recently. "To mitigate the risk," she said, "there had to be a way of making sure that if we were both arrested, the story didn't stop."

Of the three people who got copies, one remains unknown to us. Another asked to remain private. The third was Trevor Timm, a lawyer, journalist, and activist who is the executive director of the Freedom of the Press Foundation.

Trevor received a nondescript package in 2013, with the return address of somebody he knew. "Nobody said a package was coming for me," he told us. The contents were accompanied by a note from Laura, which explained that she and Glenn Greenwald were working on a big story and asked if Trevor could hold on to the enclosed material. She also cautioned him: "Don't give it to anybody except Glenn, and only if Glenn asks for it in person."

Trevor put the package in a safe place. At the time, he was overwhelmed with work, and soon forgot about the whole business — until the *Guardian* unveiled its first story from the Snowden archive.

He was, as he later recalled, "shoulder deep in the Manning trial on June fifth. Then it suddenly dawned on me. 'Oh, shit. *This* is the story.'" Soon after, he spoke on the phone with Greenwald, who indicated that there were many more stories to come.

There were other people who had also been critical to the operation, even if they hadn't received a copy of the material. On January 11, 2013, for example, an Electronic Freedom Foundation staff technologist named Micah Lee received an anonymous message that had been encrypted using PGP (Pretty Good Privacy). Such messages require the recipient's "key" — a string of code — to open them. Otherwise, they are nothing but a nonsensical sequence of numbers and characters. Micah's PGP key was public, which is why the anonymous sender chose to get in touch with him.

The sender turned out to be Snowden, who would contact Laura for the first time just days later. He was seeking a verified PGP key for Laura as well as her email address — and had noticed that both Micah and Laura were involved with the Freedom of the Press Foundation. "He figured that since I knew her, I probably had it," Micah told us recently.

From the start, he said, their communication was flawed. Snowden had initially forgotten to provide his own PGP key, which meant that Micah's reply couldn't be encrypted. "Everything wasn't perfect," Micah said, recalling such missteps. "But there was no red flag, and I've gotten lots of emails from random anonymous people. I did pretty well, considering that I had no idea what the hell was going on. I kept switching anonymous identities. When I first talked to him, I made a new anonymous identity, and then when he got to Hong Kong, I switched. And when he left Hong Kong, I switched again."

Micah communicated using Tails on a USB flash drive. When the Snowden story broke in June 2013, Micah kept the USB stick on his person at all times, even when he went jogging, for fear that the authorities would show up at his home.

Laura was "totally smart," he said, to keep the players separate. "Let's say that my house had gotten raided. I wouldn't be able to tell them about you guys. I didn't know you guys. It makes a lot of sense."

Did he think the NSA was watching him?

“Obviously. They’re watching everybody.”

TURNKEY TYRANNY

On August 9, 2013, President Obama addressed the Snowden revelations in a press conference, and assured the public that they had nothing to fear from the NSA’s data-collection apparatus: “I am comfortable that the program currently is not being abused.” George W. Bush had issued similar reassurances long before the scope of such programs was clear. *Trust us*, was the essential message.

It was hard enough to do so back then. It is even harder in the era of Donald Trump, a man who has significantly different interests and values than Obama (and, for that matter, Bush). In a video posted by the *Guardian* on June 9, 2013, Snowden seemed strangely prescient about what was to come. “There will be a time,” he said, “when policies will change”:

The only thing that restricts the activities of the surveillance state are policy. Even our agreements with other sovereign governments. We consider that to be a stipulation of policy rather than a stipulation of law. And because of that, a new leader will be elected. They’ll flip the switch, say that because of the crisis, because of the dangers that we face in the world, you know, some new and unpredicted threat, we need more authority. We need more power. And there will be nothing the people can do at that point to oppose it, and it will be turnkey tyranny.

Ben Wizner, who is the director of the A.C.L.U.’s Speech, Privacy, and Technology Project as well as Snowden’s attorney, was also impressed by how precisely his client had anticipated the potential dangers of a Trump presidency. Snowden’s scenario of turnkey tyranny “probably struck people as exotic and paranoid at the time, even though he was delivering it so earnestly. It was anticipating the moment that we are in right now.” Wizner credited the public with actually paying attention to Snowden’s warnings. “Because he wasn’t ignored, we’re better prepared for this moment.”

Wizner cited some promising developments. “For the first time in a generation,” he pointed out, “the courts have gotten involved in assessing the legality of surveillance programs.” After decades of expanding the surveillance authority of the intelligence agencies, Congress has begun to rein them in again. Technology companies, too, have begun to secure their products and build end-to-end encryption into communications software.

Still, laws can be overturned, especially when Republicans control the White House and both houses of Congress. Trump picked Mike Pompeo to head the CIA, and the Tea Party stalwart has indicated that he would like to see the minimal post-Snowden reforms repealed. In 2016, he coauthored a *Wall Street Journal* op-ed in which he wrote,

Congress should pass a law re-establishing collection of all metadata, and combining it with publicly available financial and lifestyle information into a comprehensive, searchable database.

In this environment, it’s more vital than ever that whistle-blowers and the press be ready. In numerous ways, things are better for leakers than they were in 2013. “Part of what we do at the Freedom of the Press Foundation,” said Trevor Timm, “is make it easier for the next Edward

Snowden.” To that end, the foundation raised \$60,000 to create the SecureDrop project, an open-source whistle-blower submission system now used by some thirty news organizations, including the Associated Press, the *Washington Post*, *Vice*, and *The New Yorker*.

According to Trevor, there has been an “explosion of demand” for SecureDrop since Trump’s election. He added that the F.P.F. has raised several hundred thousand dollars of additional funding for the project, which now has five full-time employees. “There is a new urgency among media organizations to use tools like this to facilitate secure leaking.”

The *New York Times* has meanwhile made its PGP key public and urged potential leakers to send in material via the U.S. mail. Indeed, when a sheaf of Trump’s tax documents turned up at the *Times*, it arrived the old-fashioned way, in a reporter’s mail slot.



In the months following Trump’s election, downloads of Signal, an encrypted-messaging app, also jumped more than 400 percent. There’s no way to estimate how many of those users are journalists, but Micah Lee recommends the app to sources and reporters alike, even if they were not yet transmitting sensitive material. “Using the tools *before* you need the tools is super important,” he said. “Because nobody ever knows when they are going to be dropped into a situation like this.”

The battle to maintain our constitutional right to privacy isn’t the exclusive realm of cyberninjas and hackers, journalists and government officials. These are critical issues, relevant to everyone. In the era of smartphone video, it’s not uncommon for ordinary citizens to find themselves possessing sensitive material that the state might want to suppress. This happened in the wake of the 2014

police shooting of Michael Brown in Ferguson, Missouri, when several people who filmed the ensuing protests were arrested. Since then, police officers have harassed and detained smartphone-wielding bystanders all over the country.

Anyone interested in the issue can advance it in a small way by normalizing the use of encrypted communication. “We should all be sending encrypted cat pictures to each other,” Laura told a group of journalists in Berlin in 2014. If everyone participated, she argued, it would overwhelm the NSA’s ability to monitor American citizens.

Meanwhile, the mass adoption of encryption already appears to be having an impact. In March, WikiLeaks released CIA documents detailing techniques for hacking into individual smartphones. For privacy advocates, this came as a backhanded compliment. It meant that secure-communications tools like Signal had proved their worth, forcing agents to resort to more cumbersome surveillance strategies, which often require access to targeted cell phones for the purpose of installing malware.

MAHARIDGE

In the summer of 2014, Laura and I met in Berlin at a rooftop restaurant in a tall building that had once been a Jewish-owned department store. After the Nazis took it over, the place had housed the Hitler Youth, and later some senior officials of the Stasi, which spied on East Germans under the Communist government. It was a fitting place, then, to discuss the NSA's surveillance of the American public.

We had a nearly 360-degree view. All of Berlin surrounded us in the long dusk. To the west was the Fernsehturm, the lofty television tower near the Alexanderplatz. Laura and I were continuing a conversation I had begun the year before, via Tails, when she was in Berlin and I was in New York. The topic: the box. Jess and I had been aching to tell the story of that brittle summer of 2013. We hoped to fill in the historical record and help to humanize the narrative around a monumental leak. I was also aware that I had pulled Jess into a certifiably crazy situation without her knowledge, and I wanted to help her make sense of it all.

Laura wasn't ready. "There are still many risks right now," she said.

I didn't see how the story of the box would incur risk. She said the big obstacle was "source protection." I wondered if there was a way to assuage that concern, and we went around and around. I reminded her that Obama had fulfilled few of his promises about transparency, and that more leaks were likely to come. "Others have to learn from what happened," I insisted, to no avail.

But two years later, Laura dined in New York with Jess and Trevor and me, and halfway through the meal she surprised us by announcing it was time. Why now? She said the danger level had lessened and the big stories were already out. Also, she seemed to recognize the importance of getting it all down for posterity, and even agreed to talk to us about those tumultuous months.

From Laura's perspective, I've surely said too much about our personal involvement, but there's no other way to tell the story. It explains her motive. "You were the person I trusted to be able to do what I needed to do," she told me recently. "There was nobody else I could ask." She also reminded me that she had asked me more than once to travel to Hong Kong with her to help break the Snowden story.

"I invited you," she said. "So you have to include that. Don't censor it."

I won't. But do I regret having declined her invitation to Hong Kong? No. In part, I had been dealing with profound depression over a book I had written about my father. But to a greater degree, it simply wasn't my story. It belonged to her and Greenwald, not to mention the other people whom she entrusted to tell it. Some friends are befuddled to this day that I didn't go on that trip to meet Snowden — that I didn't transform myself into a major player in what turned out to be a history-making drama — but I'm happy with my role in the story.

Besides, it wasn't just journalism. It was life.

BRUDER

For the past four years, every time I heard that a new and comprehensive account of the Snowden leaks was looming, I wondered, Will the box be in there? And then I thought, Better go cover the picnic table again.

Until now, however, it has been absent from the historical narrative. Greenwald's book *No Place to Hide* makes no mention of it. Neither does Laura's film *Citizenfour*. Despite my anxieties, I always

hoped it would come out, because to me, it reveals the humanness — the flaws and messiness bound up with idealism and courage — of the whole endeavor.

There's no way to know what Snowden was thinking when he wrote down his actual street in Waipahu and the pseudonym B. Manning. I tried puzzling it out with a few people close to the situation. Why would such a smart guy have risked exposing himself and others, just to crack a joke?

"He's not an idiot," I told one of them.

"But he was in that instance," came the reply.

A couple of others guessed that at the crucial juncture of sending the box, Snowden may have felt like he was on what amounted to a suicide mission. Dale and I hoped to answer this question, and maybe a good many others, by talking to the man himself. Over the course of six months, we made three separate requests to speak with Snowden. Two went unanswered. With the third, we heard back through an intermediary. "I'm not sure I'm ready to tell my side of that part of the timeline yet," Snowden wrote.

One of the requests went through Ben Wizner, his attorney. Weeks after sending it, we sat with Wizner in his office in the A.C.L.U.'s Manhattan headquarters. There had been no reply. We still thought we might get an audience with the man in Moscow. After all, in the years since Snowden came forward, he's granted numerous interviews. He's spoken with everyone from Brian Lehrer to John Oliver to Katie Couric to Oliver Stone. Wizner wasn't optimistic, though.

"I think it's unlikely," he said. "One of the few things he has left is *his* side of the story, which he's never told. It's a very valuable thing. And he has to write a book someday."

Dale reiterated our pitch. "What we wanted was, again, specific to the leaking process. How the analog part happened. That's really critical for other whistle-blowers."

Wizner frowned. "There's no way he's going to talk to you about that. No, no, no. If he had wanted that information out there, it would have been out there a long time ago."

He paused, and when he spoke again, there was a trace of sarcasm. "I mean, *really*. You can't think you're the first ones to be interested in that!"

All of which is to say, details would not be forthcoming from Snowden anytime soon. But I do look forward to reading his book.

THE TREE

It was a calm, blue-sky day last summer, three years after the copy of the Snowden material had been cached in the Douglas fir. We carried a heavy fiberglass ladder into the forest and propped it against the tree. There was no worry about being spied on by drones or a satellite. Everything had worked out. Laura, Greenwald, and Snowden were safe, at least for now. So were the other players.

Then one of us made a joke: what if the material was gone? Suddenly, the day didn't seem so sunny in the deep shade of the ancient tree. We ascended the ladder.

For some reason, Douglas firs that grow close to the ocean have much stouter branches than their inland counterparts. Once the ladder ended, it was easy to climb from branch to branch up to where

the material was located. A bird had built a nest on top of the sealed container. Happily, the nest was empty: breeding season had passed. We opened the container. The item was inside.

We remained in the tree for a while. There was a view of the Pacific and the studio where Laura cut some of her NSA mini-documentary for the *Times*, which Snowden had watched in late 2012 — indeed, it was one of the reasons he cited for contacting her in the first place. In a way, then, as we perched among the branches, we were where things both began and ended for our supporting roles in the Snowden narrative.

We brought the material down. Now it's hidden somewhere else — off Dale's property in a location known only to him. Why keep it at all? There is always the possibility that it could be seized as evidence. Yet we hang on to such items. The box and those copies of what it contained are artifacts of a critical moment in American history, especially for anyone who cares about the Fourth Amendment and government abuse of power. Maybe it's human nature to focus on the tension and emotion from the summer of 2013: we are definitely reliving it now, by telling this story. But when we look at the pictures we took as we climbed down from the tree, in most of them, we're smiling.

• *You are currently viewing this article as a guest. If you are a subscriber, please sign in. If you aren't, please subscribe below and get access to the entire Harper's archive for only \$45.99/year. Or purchase this issue on your [iOS](#) or [Android](#) devices for \$6.99.*

• = Subscribers only.

Sign in [here](#).

Subscribe [here](#).

- [SIGN IN to access Harper's Magazine](#)
- [Need help?](#)

SIGN IN to access *Harper's Magazine*

[Close](#) X

Email
●●●●●●●●
Log - in

Need to create a login? Want to change your email address or password? Forgot your password?

1. Sign in to [Customer Care](#) using your account number or postal address.
2. Select Email/Password Information.
3. Enter your new information and click on Save My Changes.

Subscribers can find additional help [here](#). Not a subscriber? [Subscribe today!](#)

- TAGS
- [\[21st century\]](#)
- [\[Dale Maharidge\]](#)
- [\[Domestic intelligence\]](#)
- [\[Edward J. Snowden\]](#)
- [\[Electronic surveillance\]](#)