NEW YORK TIMES BESTSELLER

NO PLACE TO HIDE

Edward Snowden, the NSA, and the U.S. Surveillance State

"Impassioned...gripping...Greenwald amplifies our understanding of the N.S.A.'s sweeping ambitions...and delivers a fierce argument in defense of the right of privacy." —Michiko Kakutani, *The New York Times*

GLENN GREENWALD

PICADOR

Metropolitan Books
Henry Holt and Company, LLC
Publishers since 1866
175 Fifth Avenue
New York, New York 10010
www.henryholt.com

ISBN: 978-1-62779-073-4
Library of Congress Control Number: 2014932888

Henry Holt books are available for special promotions and
premiums. For details contact: Director, Special Markets.

First Edition 2014

Designed by Kelly S. Too

Printed in the United States of America
1 3 5 7 9 10 8 6 4 2

This book is dedicated to all those who have sought to shine a light on the US government's secret mass surveillance systems, particularly the courageous whistle-blowers who have risked their liberty to do so.

The United States government has perfected a technological capability that enables us to monitor the messages that go through the air. . . . That capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide.

—Senator Frank Church, Chair, Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975

CONTENTS

1

CONTACT

On December 1, 2012, I received my first communication from Edward Snowden, although I had no idea at the time that it was from him.

The contact came in the form of an email from someone calling himself Cincinnatus, a reference to Lucius Quinctius Cincinnatus, the Roman farmer who, in the fifth century BC, was appointed dictator of Rome to defend the city against attack. He is most remembered for what he did after vanquishing Rome's enemies: he immediately and voluntarily gave up political power and returned to farming life. Hailed as a "model of civic virtue," Cincinnatus has become a symbol of the use of political power in the public interest and the worth of limiting or even relinquishing individual power for the greater good.

The email began: "The security of people's communications is very important to me," and its stated purpose was to urge me to begin using PGP encryption so that "Cincinnatus" could communicate things in which, he said, he was certain I would be interested. Invented in 1991, PGP stands for "pretty good privacy." It has been developed into a sophisticated tool to shield email and other forms of online communications from surveillance and hacking.

The program essentially wraps every email in a protective shield, which is a code composed of hundreds, or even thousands, of random

numbers and case-sensitive letters. The most advanced intelligence agencies around the world—a class that certainly includes the National Security Agency—possess password-cracking software capable of one billion guesses per second. But so lengthy and random are these PGP encryption codes that even the most sophisticated software requires many years to break them. People who most fear having their communications monitored, such as intelligence operatives, spies, human rights activists, and hackers, trust this form of encryption to protect their messages.

In this email, "Cincinnatus" said he had searched everywhere for my PGP "public key," a unique code set that allows people to receive encrypted email, but could not find it. From this, he concluded that I was not using the program and told me, "That puts anyone who communicates with you at risk. I'm not arguing that every communication you are involved in be encrypted, but you should at least provide communicants with that option."

"Cincinnatus" then referenced the sex scandal of General David Petraeus, whose career-ending extramarital affair with journalist Paula Broadwell was discovered when investigators found Google emails between the two. Had Petraeus encrypted his messages before handing them over to Gmail or storing them in his drafts folder, he wrote, investigators would not have been able to read them. "Encryption matters, and it is not just for spies and philanderers." Installing encrypted email, he said, "is a critically-necessary security measure for anyone who wishes to communicate with you."

To motivate me to follow his advice, he added, "There are people out there you would like to hear from who will never be able to contact you without knowing their messages cannot be read in transit."

Then he offered to help me install the program: "If you need any help at all with this, please let me know, or alternately request help on Twitter. You have many technically-proficient followers who are willing to offer immediate assistance." He signed off: "Thank you. C."

Using encryption software was something I had long intended to do. I had been writing for years about WikiLeaks, whistle-blowers, the hacktivist collective known as Anonymous, and related topics, and had also communicated from time to time with people inside the US national

security establishment. Most of them are very concerned about the security of their communications and preventing unwanted monitoring. But the program is complicated, especially for someone who had very little skill in programming and computers, like me. So it was one of those things I had never gotten around to doing.

C.'s email did not move me to action. Because I had become known for covering stories the rest of the media often ignores, I frequently hear from all sorts of people offering me a "huge story," and it usually turns out to be nothing. And at any given moment I am usually working on more stories than I can handle. So I need something concrete to make me drop what I'm doing in order to pursue a new lead. Despite the vague allusion to "people out there" I "would like to hear from," there was nothing in C.'s email that I found sufficiently enticing. I read it but did not reply.

Three days later, I heard from C. again, asking me to confirm receipt of the first email. This time I replied quickly. "I got this and am going to work on it. I don't have a PGP code, and don't know how to do that, but I will try to find someone who can help me."

C. replied later that day with a clear, step-by-step guide to the PGP system: Encryption for Dummies, in essence. At the end of the instructions, which I found complex and confusing, mostly due to my own ignorance, he said these were just "the barest basics. If you can't find anyone to walk you through installation, generation, and use," he added, "please let me know. I can facilitate contact with people who understand crypto almost anywhere in the world."

This email ended with more a pointed sign-off: "Cryptographically yours, Cincinnatus."

Despite my intentions, I never created the time to work on encryption. Seven weeks went by, and my failure to do this weighed a bit on my mind. What if this person really did have an important story, one I would miss just because I failed to install a computer program? Apart from anything else, I knew encryption might be valuable in the future, even if Cincinnatus turned out to have nothing of interest.

On January 28, 2013, I emailed C. to say that I would get someone to help me with encryption and hopefully would have it done within the next day or so.

C. replied the next day: "That's great news! If you need any further help or have questions in the future, you will always be welcome to reach out. Please accept my sincerest thanks for your support of communications privacy! Cincinnatus."

But yet again, I did nothing, consumed as I was at the time with other stories, and still unconvinced that C. had anything worthwhile to say. There was no conscious decision to do nothing. It was simply that on my always too-long list of things to take care of, installing encryption technology at the behest of this unknown person never became pressing enough for me to stop other things and focus on it.

C. and I thus found ourselves in a Catch-22. He was unwilling to tell me anything specific about what he had, or even who he was and where he worked, unless I installed encryption. But without the enticement of specifics, it was not a priority to respond to his request and take the time to install the program.

In the face of my inaction, C. stepped up his efforts. He produced a ten-minute video entitled *PGP for Journalists*. Using software that generates a computer voice, the video instructed me in an easy, step-by-step fashion how to install encryption software, complete with charts and visuals.

Still I did nothing. It was at that point that C., as he later told me, become frustrated. "Here am I," he thought, "ready to risk my liberty, perhaps even my life, to hand this guy thousands of Top Secret documents from the nation's most secretive agency—a leak that will produce dozens if not hundreds of huge journalistic scoops. And he can't even be bothered to install an encryption program."

That's how close I came to blowing off one of the largest and most consequential national security leaks in US history.

The next I heard of any of this was ten weeks later. On April 18, I flew from my home in Rio de Janeiro to New York, where I was scheduled to give some talks on the dangers of government secrecy and civil liberties abuses done in the name of the War on Terror.

On landing at JFK Airport, I saw that I had an email message from

Laura Poitras, the documentary filmmaker, which read: "Any chance you'll be in the US this coming week? I'd love to touch base about something, though best to do in person."

I take seriously any message from Laura Poitras. One of the most focused, fearless, and independent individuals I've ever known, she has made film after film in the riskiest of circumstances, with no crew or the support of a news organization, just a modest budget, one camera, and her determination. At the height of the worst violence of the Iraq War, she ventured into the Sunni Triangle to make *My Country, My Country*, an unflinching look at life under US occupation that was nominated for an Academy award.

For her next film, *The Oath*, Poitras traveled to Yemen, where she spent months following two Yemeni men—Osama bin Laden's bodyguard as well as his driver. Since then, Poitras has been working on a documentary about NSA surveillance. The three films, conceived as a trilogy about US conduct during the War on Terror, made her a constant target of harassment by government authorities every time she entered or left the country.

Through Laura, I learned a valuable lesson. By the time we first met, in 2010, she had been detained in airports by the Department of Homeland Security more than three dozen times as she entered the United States—interrogated, threatened, her materials seized, including her laptop, cameras, and notebooks. Yet she repeatedly decided not to go public with the relentless harassment, fearing that the repercussions would make her work impossible. That changed after an unusually abusive interrogation at Newark Liberty International Airport. Laura had had enough. "It's getting worse, not better, from my being silent." She was ready for me to write about it.

The article I published in the online political magazine *Salon* detailing the constant interrogations to which Poitras had been subjected received substantial attention, drawing statements of support and denunciations of the harassment. The next time Poitras flew out of the United States after the article ran, there was no interrogation and she did not have her materials seized. Over the next couple of months, there was no harassment. For the first time in years, Laura was able to travel freely.

The lesson for me was clear: national security officials do not like the light. They act abusively and thuggishly only when they believe they are safe, in the dark. Secrecy is the linchpin of abuse of power, we discovered, its enabling force. Transparency is the only real antidote.

At JFK, reading Laura's email, I replied immediately: "Actually, just got to the US this morning. . . . Where are you?" We arranged a meeting for the next day, in the lobby at my hotel in Yonkers, a Marriott, and found seats in the restaurant, At Laura's insistence, we moved tables twice before beginning our conversation to be sure that nobody could hear us. Laura then got down to business. She had an "extremely important and sensitive matter" to discuss, she said, and security was critical.

Since I had my cell phone with me, Laura asked that I either remove the battery or leave it in my hotel room. "It sounds paranoid," she said, but the government has the capability to activate cell phones and laptops remotely as eavesdropping devices. Powering off the phone or laptop does not defeat the capability: only removing the battery does. I'd heard this before from transparency activists and hackers but tended to write it off as excess caution, but this time I took it seriously because it came from Laura. After discovering that the battery on my cell phone could not be removed, I took it back to my room, then returned to the restaurant.

Now Laura began to talk. She had received a series of anonymous emails from someone who seemed both honest and serious. He claimed to have access to some extremely secret and incriminating documents about the US government spying on its own citizens and on the rest of the world. He was determined to leak these documents to her and had specifically requested that she work with me on releasing and reporting on them. I made no connection at the time to the long-since-forgotten emails I had received from Cincinnatus months earlier. They had been parked at the back of my mind, out of view.

Laura then pulled several pages out of her purse from two of the emails sent by the anonymous leaker, and I read them at the table from start to finish. They were riveting.

The second of the emails, sent weeks after the first, began: "Still here."

With regard to the question at the forefront of my mind—when would he be ready to furnish documents?—he had written, "All I can say is 'soon.'"

After urging her to always remove batteries from cell phones before talking about sensitive matters—or, at least, to put the phones in the freezer, where their eavesdropping capability would be impeded—the leaker told Laura that she should work with me on these documents. He then got to the crux of what he viewed as his mission:

> The shock of this initial period [after the first revelations] will provide the support needed to build a more equal internet, but this will not work to the advantage of the average person unless science outpaces law. By understanding the mechanisms through which our privacy is violated, we can win here. We can guarantee for all people equal protection against unreasonable search through universal laws, but only if the technical community is willing to face the threat and commit to implementing over-engineered solutions. In the end, we must enforce a principle whereby the only way the powerful may enjoy privacy is when it is the same kind shared by the ordinary: one enforced by the laws of nature, rather than the policies of man.

"He's real," I said when I finished reading. "I can't explain exactly why, but I just feel intuitively that this is serious, that he's exactly who he says he is."

"So do I," Laura replied. "I have very little doubt."

Reasonably and rationally, Laura and I knew that our faith in the leaker's veracity might have been misplaced. We had no idea who was writing to her. He could have been anyone. He could have been inventing the entire tale. This also could have been some sort of plot by the government to entrap us into collaborating with a criminal leak. Or perhaps it had come from someone who sought to damage our credibility by passing on fraudulent documents to publish.

We discussed all these possibilities. We knew that a 2008 secret report by the US Army had declared WikiLeaks an enemy of the state and proposed ways to "damage and potentially destroy" the organization. The report (ironically leaked to WikiLeaks) discussed the possibility of pass-

ing on fraudulent documents. If WikiLeaks published them as authentic, it would suffer a serious blow to its credibility.

Laura and I were aware of all the pitfalls but we discounted them, relying instead on our intuition. Something intangible yet powerful about those emails convinced us that their author was genuine. He wrote out of a belief in the dangers of government secrecy and pervasive spying; I instinctively recognized his political passion. I felt a kinship with our correspondent, with his worldview, and with the sense of urgency that was clearly consuming him.

Over the past seven years, I had been driven by the same conviction, writing almost on a daily basis about the dangerous trends in US state secrecy, radical executive power theories, detention and surveillance abuses, militarism, and the assault on civil liberties. There is a particular tone and attitude that unites journalists, activists, and readers of mine, people who are equally alarmed by these trends. It would be difficult, I reasoned, for someone who did not truly believe and feel this alarm to replicate it so accurately, with such authenticity.

In one of the last passages of Laura's emails, her correspondent wrote that he was completing the final steps necessary to provide us with the documents. He needed another four to six weeks, and we should wait to hear from him. He assured us that we would.

Three days later, Laura and I met again, this time in Manhattan, and with another email from the anonymous leaker, in which he explained why he was willing to risk his liberty, to subject himself to the high likelihood of a very lengthy prison term, in order to disclose these documents. Now I was even more convinced: our source was for real, but as I told my partner, David Miranda, on the flight home to Brazil, I was determined to put the whole thing out of my mind. "It may not happen. He could change his mind. He could get caught." David is a person of powerful intuition, and he was weirdly certain. "It's real. He's real. It's going to happen," he declared. "And it's going to be huge."

After returning to Rio, I heard nothing for three weeks. I spent almost no time thinking about the source because all I could do was wait. Then,

on May 11, I received an email from a tech expert with whom Laura and I had worked in the past. His words were cryptic but his meaning clear: "Hey Glenn, I'm following up with learning to use PGP. Do you have an address I can mail you something to help you get started next week?"

I was sure that the something he wanted to send was what I needed to begin working on the leaker's documents. That, in turn, meant Laura had heard from our anonymous emailer and received what we had been waiting for.

The tech person then sent a package via Federal Express, scheduled to arrive in two days. I did not know what to expect: a program, or the documents themselves? For the next forty-eight hours, it was impossible to focus on anything else. But on the day of scheduled delivery, 5:30 p.m. came and went and nothing arrived. I called FedEx and was told that the package was being held in customs for "unknown reasons." Two days went by. Then five. Then a full week. Every day FedEx said the same thing—that the package was being held in customs, for reasons unknown.

I briefly entertained the suspicion that some government authority—American, Brazilian, or otherwise—was responsible for this delay because they knew something, but I held on to the far likelier explanation that it was just one of those coincidental bureaucratic annoyances.

By this point, Laura was very reluctant to discuss any of this by phone or online, so I didn't know what exactly was in the package.

Finally, roughly ten days after the package had been sent to me, FedEx delivered it. I tore open the envelope and found two USB thumb drives, along with a typewritten note containing detailed instructions for using various computer programs designed to provide maximum security, as well as numerous passphrases to encrypted email accounts and other programs I had never heard of.

I had no idea what all this meant. I had never heard of these specific programs before, although I knew about passphrases, basically long passwords containing randomly arranged case-sensitive letters and punctuation, designed to make them difficult to crack. With Poitras deeply reluctant to talk by phone or online, I was still frustrated: finally in possession of what I was waiting for, but with no clue where it would lead me.

I was about to find out, from the best possible guide.

The day after the package arrived, during the week of May 20, Laura told me we needed to speak urgently, but only through OTR (off-the-record) chat, an encrypted instrument for talking online securely. I had used OTR previously, and managed to install the chat program, signed up for an account, and added Laura's user name to my "buddy list." She showed up instantly.

I asked about whether I now had access to the secret documents. They would only come to me from the source, she told me, not from her. Laura then added some startling new information, that we might have to travel to Hong Kong immediately, to meet our source. Now I was baffled. What was someone with access to top secret US government documents doing in Hong Kong? I had assumed that our anonymous source was in Maryland or northern Virginia. What did Hong Kong have to do with any of this? I was willing to travel anywhere, of course, but I wanted more information about why I was going. But Laura's inability to speak freely forced us to postpone that discussion.

She asked whether I'd be willing to travel to Hong Kong within the next few days. I wanted to be certain that this would be worthwhile, meaning: Had she obtained verification that this source was real? She cryptically replied, "Of course, I wouldn't ask you to go to Hong Kong if I hadn't." I assumed this meant she had received some serious documents from the source.

But she also told me about a brewing problem. The source was upset by how things had gone thus far, particularly about a new turn: the possible involvement of the *Washington Post*. Laura said it was critical that I speak to him directly, to assure him and placate his growing concerns.

Within an hour, the source himself emailed me.

This email came from Verax@[redacted]. *Verax* means "truth teller" in Latin. The subject line read, "Need to talk."

"I've been working on a major project with a mutual friend of ours," the email began, letting me know that it was he, the anonymous source, clearly referring to his contacts with Laura.

"You recently had to decline short-term travel to meet with me. You need to be involved in this story," he wrote. "Is there any way we can talk on short notice? I understand you don't have much in the way of secure

infrastructure, but I'll work around what you have." He suggested that we speak via OTR and provided his user name.

I was uncertain what he had meant about "declining short-term travel": I had expressed confusion about why he was in Hong Kong but certainly hadn't refused to go. I chalked that up to miscommunication and replied immediately. "I want to do everything possible to be involved in this," I told him, suggesting that we talk right away on OTR. I added his user name to my OTR buddy list and waited.

Within fifteen minutes, my computer sounded a bell-like chime, signaling that he had signed on. Slightly nervous, I clicked on his name and typed "hello." He answered, and I found myself speaking directly to someone who I assumed had, at that point, revealed a number of secret documents about US surveillance programs and who wanted to reveal more.

Right off the bat, I told him I was absolutely committed to the story. "I'm willing to do what I have to do to report this," I said. The source—whose name, place of employment, age, and all other attributes were still unknown to me—asked if I would come to Hong Kong to meet him. I did not ask why he was in Hong Kong; I wanted to avoid appearing to be fishing for information.

Indeed, from the start I decided I would let him take the lead. If he wanted me to know why he was in Hong Kong, he would tell me. And if he wanted me to know what documents he had and planned to provide me, he would tell me that, too. This passive posture was difficult for me. As a former litigator and current journalist, I'm accustomed to aggressive questioning when I want answers, and I had hundreds of things I wanted to ask.

But I assumed his situation was delicate. Whatever else was true, I knew that this person had resolved to carry out what the US government would consider a very serious crime. It was clear from how concerned he was with secure communications that discretion was vital. And, I reasoned,—since I had so little information about whom I was talking to, about his thinking, his motives and fears—that caution and restraint on my part were imperative. I did not want to scare him off, so I forced myself to let the information come to me rather than trying to grab it.

"Of course I'll come to Hong Kong," I said, still having no idea why he was there, of all places, or why he wanted me to go there.

We spoke online that day for two hours. His first concern was what was happening with some of the NSA documents that, with his consent, Poitras had talked about to a *Washington Post* reporter, Barton Gellman. The documents pertained to one specific story about a program called PRISM, which allowed the NSA to collect private communications from the world's largest Internet companies, including Facebook, Google, Yahoo!, and Skype.

Rather than report the story quickly and aggressively, the *Washington Post* had assembled a large team of lawyers who were making all kinds of demands and issuing all sorts of dire warnings. To the source, this signaled that the *Post*, handed what he believed was an unprecedented journalistic opportunity, was being driven by fear rather than conviction and determination. He was also livid that the *Post* had involved so many people, afraid that these discussions might jeopardize his security.

"I don't like how this is developing," he told me. "I had wanted someone else to do this one story abut PRISM so you could focus on the broader archive, especially the mass domestic spying, but now I really want you to be the one to report this. I've been reading you a long time," he said, "and I know you'll be aggressive and fearless in how you do this."

"I'm ready and eager," I told him. "Let's decide now what I need to do."

"The first order of business is for you to get to Hong Kong," he said. He returned to that again and again: *come to Hong Kong immediately.*

The other significant topic we discussed in that first online conversation was his goal. I knew from the emails Laura had shown me that he felt compelled to tell the world about the massive spying apparatus the US government was secretly building. But what did he hope to achieve?

"I want to spark a worldwide debate about privacy, Internet freedom, and the dangers of state surveillance," he said. "I'm not afraid of what will happen to me. I've accepted that my life will likely be over from my doing this. I'm at peace with that. I know it's the right thing to do."

He then said something startling: "I want to identify myself as the person behind these disclosures. I believe I have an obligation to explain why I'm doing this and what I hope to achieve." He told me he had written a document that he wanted to post on the Internet when he outed himself as the source, a pro-privacy, anti-surveillance manifesto for peo-

ple around the world to sign, showing that there was global support for protecting privacy.

Despite the near-certain costs of outing himself—a lengthy prison term if not worse—he was, the source said again and again, "at peace" with those consequences. "I only have one fear in doing all of this," he said, which is "that people will see these documents and shrug, that they'll say, 'we assumed this was happening and don't care.' The only thing I'm worried about is that I'll do all this to my life for nothing."

"I seriously doubt that will happen," I assured him, but I wasn't convinced I really believed that. I knew from my years of writing about NSA abuses that it can be hard to generate serious concern about secret state surveillance: invasion of privacy and abuse of power can be viewed as abstractions, ones that are difficult to get people to care about viscerally. What's more, the issue of surveillance is invariably complex, making it even harder to engage the public in a widespread way.

But this felt different. The media pays attention when top secret documents are leaked. And the fact that the warning was coming from someone on the inside of the national security apparatus—rather than an American Civil Liberties Union lawyer or a civil liberties advocate—surely meant that it would have added weight.

That night, I talked to David about going to Hong Kong. I was still reluctant to drop all of my work to fly to the other side of the world to meet someone I knew nothing about, not even his name, particularly since I had no real evidence that he was who he said he was. It could be a complete waste of time—or entrapment or some other weird plot.

"You should tell him that you want to see a few documents first to know that he's serious and that this is worth it for you," David suggested.

As usual, I took his advice. When I signed on to OTR the next morning, I said I was planning to leave for Hong Kong within days but first wanted to see some documents so that I understood the types of disclosures he was prepared to make.

To do that, he told me again to install various programs. I then spent a couple of days online as the source walked me through, step by step, how to install and use each program, including, finally, PGP encryption. Knowing that I was a beginner, he exhibited great patience, literally on

the level of "Click the blue button, now press OK, now go to the next screen."

I kept apologizing for my lack of proficiency, for having to take hours of his time to teach me the most basic aspects of secure communication. "No worries," he said, "most of this makes little sense. And I have a lot of free time right now."

Once the programs were all in place, I received a file containing roughly twenty-five documents: "Just a very small taste: the tip of the tip of the iceberg," he tantalizingly explained.

I un-zipped the file, saw the list of documents, and randomly clicked on one of them. At the top of the page in red letters, a code appeared: "TOP SECRET//COMINT/NOFORN/."

This meant the document had been legally designated top secret, pertained to communications intelligence (COMINT), and was not for distribution to foreign nationals, including international organizations or coalition partners (NOFORN). There it was with incontrovertible clarity: a highly confidential communication from the NSA, one of the most secretive agencies in the world's most powerful government. Nothing of this significance had ever been leaked from the NSA, not in all the six-decade history of the agency. I now had a couple dozen such items in my possession. And the person I had spent hours chatting with over the last two days had many, many more to give me.

That first document was a training manual for NSA officials to teach analysts about new surveillance capabilities. It discussed in broad terms the type of information the analysts could query (email addresses, IP [Internet protocol] locator data, telephone numbers) and the type of data they would receive in response (email content, telephone "metadata," chat logs). Basically, I was eavesdropping on NSA officials as they instructed their analysts on how to listen in on their targets.

My heart was racing. I had to stop reading and walk around my house a few times to take in what I had just seen and calm myself enough to focus on reading the files. I went back to my laptop and randomly clicked on the next document, a top secret PowerPoint presentation, entitled "PRISM/US-984XN Overview." Each page bore the logos of nine of the largest Internet companies, including Google, Facebook, Skype, and Yahoo!.

The first slides laid out a program under which the NSA had what it called "collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple." A graph displayed the dates on which each of these companies had joined the program.

Again I became so excited, I had to stop reading.

The source also said he was sending me a large file that I would be unable to access until the time was right. I decided to set aside that cryptic though significant statement for the moment, in line with my approach of letting him decide when I got information but also because I was so excited by what I had in front of me.

From the first glimpse I'd had of just these few documents, I knew two things: I needed to get to Hong Kong right away, and I would have to have substantial institutional support to do this reporting. This meant involving the *Guardian*, the newspaper and online news website that I had joined as a daily columnist only nine months earlier. Now I was about to bring them in to what I knew already would be a major explosive story.

Using Skype, I called Janine Gibson, the British editor in chief of the US edition of the *Guardian*. My agreement with the *Guardian* was that I had full editorial independence, which meant that nobody could edit or even review my articles before they ran. I wrote my pieces, and then published them directly to the Internet myself. The only exceptions to this arrangement were that I would alert them if my writing could have legal consequences for the newspaper or posed an unusual journalistic quandary. That had happened very few times in the previous nine months, only once or twice, which meant that I had had very little interaction with the *Guardian* editors.

Obviously, if any story warranted a heads-up, it was this one. Also, I knew I would need the paper's resources and support.

"Janine, I have a huge story," I plunged in. "I have a source who has access to what seems to be a large amount of top secret documents from the NSA. He's given me a few already, and they're shocking. But he says he has many, many more. For some reason, he's in Hong Kong, I have no idea why yet, and he wants me to go there to meet him and get the rest. What he's given me, what I just looked at, show some pretty shocking—"

Gibson interrupted. "How are you calling me?"

"By Skype."

"I don't think we should talk about this on the phone, and definitely not by Skype," she wisely said, and she proposed that I get on a plane to New York immediately so that we could discuss the story in person.

My plan, which I told Laura, was to fly to New York, show the documents to the *Guardian*, get them excited about the story, and then have them send me to Hong Kong to see the source. Laura agreed to meet me in New York, and then we intended to travel together to Hong Kong.

The next day, I flew from Rio to JFK on the overnight flight, and by 9:00 a.m. the following day, Friday, May 31, I had checked in to my Manhattan hotel and then met Laura. The first thing we did was go to a store to buy a laptop that would serve as my "air gapped machine," a computer that never connected to the Internet. It is much more difficult to subject an Internet-free computer to surveillance. To monitor an air gapped computer, an intelligence service such as the NSA would have to engage in far more difficult methods, such as obtaining physical access to the computer and placing a surveillance device on the hard drive. Keeping the computer close at all times helps prevent that type of invasion. I would use this new laptop to work with materials that I didn't want monitored, like secret NSA documents, without fear of detection.

I shoved my new computer into my backpack and walked the five Manhattan blocks with Laura to the *Guardian*'s Soho office.

Gibson was waiting for us when we arrived. She and I went directly into her office, where we were joined by Stuart Millar, Gibson's deputy. Laura sat outside. Gibson didn't know Laura, and I wanted us to be able to talk freely. I had no idea how the *Guardian* editors would react to what I had. I hadn't worked with them before, certainly not on anything remotely approaching this level of gravity and importance.

After I pulled up the source's files on my laptop, Gibson and Millar sat together at a table and read the documents, periodically muttering "wow" and "holy shit" and similar exclamations. I sat on a sofa and watched them read, observing the shock registering on their faces when the reality of what I possessed began to sink in. Each time they fin-

ished with one document, I popped up to show them the next one. Their amazement only intensified.

In addition to the two dozen or so NSA documents the source had sent, he had included the manifesto he intended to post, calling for signatures as a show of solidarity with the pro-privacy, anti-surveillance cause. The manifesto was dramatic and severe, but that was to be expected, given the dramatic and severe choices he had made, choices that would upend his life forever. It made sense to me that someone who had witnessed the shadowy construction of a ubiquitous system of state surveillance, with no oversight or checks, would be gravely alarmed by what he had seen and the dangers it posed. Of course his tone was extreme; he had been so alarmed that he had made an extraordinary decision to do something brave and far-reaching. I understood the reason for his tone, although I worried about how Gibson and Millar would react to reading the manifesto. I didn't want them to think we were dealing with someone unstable, particularly since, having spent many hours talking to him, I knew that he was exceptionally rational and deliberative.

My fear was quickly validated. "This is going to sound crazy to some people," Gibson pronounced.

"Some people and pro-NSA media types will say it's a bit Ted Kaczynski–ish," I agreed. "But ultimately, the documents are what matters, not him or his motives for giving them to us. And besides, anyone who does something this extreme is going to have extreme thoughts. That's inevitable."

Along with that manifesto, Snowden had written a missive to the journalists to whom he gave his archive of documents. It sought to explain his purpose and goals and predicted how he would likely be demonized:

> My sole motive is to inform the public as to that which is done in their name and that which is done against them. The U.S. government, in conspiracy with client states, chiefest among them the Five Eyes—the United Kingdom, Canada, Australia, and New Zealand—have inflicted upon the world a system of secret, pervasive surveillance from which there is no refuge. They protect their domestic systems from the oversight of citizenry through classification and lies, and shield themselves

> from outrage in the event of leaks by overemphasizing limited protections they choose to grant the governed. . . .
>
> The enclosed documents are real and original, and are offered to provide an understanding of how the global, passive surveillance system works so that protections against it may be developed. On the day of this writing, all new communications records that can be ingested and catalogued by this system are intended to be held for [] years, and new "Massive Data Repositories" (or euphemistically "Mission" Data Repositories) are being built and deployed worldwide, with the largest at the new data center in Utah. While I pray that public awareness and debate will lead to reform, bear in mind that the policies of men change in time, and even the Constitution is subverted when the appetites of power demand it. In words from history: Let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.

I instantly recognized the last sentence as a play on a Thomas Jefferson quote from 1798 that I often cited in my writing: "In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution."

After reviewing all of the documents, including Snowden's missive, Gibson and Millar were persuaded. "Basically," Gibson concluded within two hours of my arrival that morning, "you need to go to Hong Kong as soon as possible, like tomorrow, right?"

The *Guardian* was on board. My mission in New York had been accomplished. Now I knew that Gibson was committed to pursuing the story aggressively, at least for the moment. That afternoon, Laura and I worked with the *Guardian*'s travel person to get to Hong Kong as quickly as possible. The best option was a sixteen-hour non-stop flight on Cathay Pacific that left from JFK the next morning. But just as we began to celebrate our imminent meeting with the source, we ran into a complication.

At the end of the day, Gibson declared that she wanted to involve a longtime *Guardian* reporter, Ewen MacAskill, who had been at the paper for twenty years. "He's a great journalist," she said. Given the magnitude of what I was embarking on, I knew that I'd need other *Guardian* report-

ers on the story and had no objection in theory. "I'd like Ewen to go with you to Hong Kong," she added.

I didn't know MacAskill. More important, neither did the source, and as far as he knew, only Laura and I were coming to Hong Kong. And Laura, who plans everything meticulously, was also bound to be furious at this sudden change in our plans.

I was right. "No way. Absolutely not," she responded. "We can't just add some new person at the last minute. And I don't know him at all. Who has vetted him?"

I tried to explain what I thought was Gibson's motive. I didn't really know or trust the *Guardian* yet, not when it came to such a huge story, and I assumed they felt the same way about me. Given how much the *Guardian* had at stake, I reasoned that they likely wanted someone they knew very well—a longtime company man—to tell them what was going on with the source and to assure them that this story was something they should do. Besides, Gibson would need the full support and approval of the *Guardian* editors in London, who knew me even less well than she did. She probably wanted to bring in someone who could make London feel safe, and Ewen fit that bill perfectly.

"I don't care," Laura said. "Traveling with some third person, some stranger, could attract surveillance or scare the source." As a compromise, Laura suggested that they send Ewen after a few days, once we had established contact with the source in Hong Kong and built trust. "You have all the leverage. Tell them they can't send Ewen until we're ready."

I went back to Gibson with what seemed like a smart compromise, but she was determined. "Ewen can travel with you to Hong Kong, but he won't meet the source until you and Laura both say you're ready."

Clearly, Ewen coming with us to Hong Kong was crucial to the *Guardian*. Gibson would need assurances about what was happening there and a way to assuage any worries her bosses in London might have. But Laura was just as adamant that we would travel alone. "If the source surveils us at the airport and sees this unexpected third person he doesn't know, he'll freak out and terminate contact. No way." Like a State Department diplomat shuttling between Middle East adversaries in the futile hope of

brokering a deal, I went back to Gibson, who gave a vague reply designed to signal that Ewen would follow a couple of days later. Or maybe that's what I wanted to hear.

Either way, I learned from the travel person late that night that Ewen's ticket had been bought—for the next day, on the same flight. And they were sending him on that plane no matter what.

In the car on the way to the airport, Laura and I had our first and only argument. I gave her the news as soon as the car pulled out of the hotel and she exploded with anger. I was jeopardizing the entire arrangement, she insisted. It was unconscionable to bring some stranger in at this late stage. She didn't trust someone who hadn't been vetted for work on something so sensitive and she blamed me for letting the *Guardian* risk our plan.

I couldn't tell Laura that her concerns were invalid, but I did try to convince her that the *Guardian* was insistent, there was no choice. And Ewen would only meet the source when we were ready.

Laura didn't care. To placate her anger, I even offered not to go, a suggestion she instantly rejected. We sat in miserable, angry silence for ten minutes as the car was stuck in traffic on the way to JFK.

I knew Laura was right: it shouldn't have happened this way, and I broke the silence by telling her so. I then proposed that we ignore Ewen and freeze him out, pretend that he's not with us. "We're on the same side," I appealed to Laura. "Let's not fight. Given what's at stake, this won't be the last time that things happen beyond our control." I tried to persuade Laura that we should keep our focus on working together to overcome obstacles. In a short time, we returned to a state of calm.

As we arrived in the vicinity of JFK Airport, Laura pulled a thumb drive out of her backpack. "Guess what this is?" she asked with a look of intense seriousness.

"What?"

"The documents," she said. "All of them."

Ewen was already at our gate when we arrived. Laura and I were cordial but cold, ensuring that he felt excluded, that he had no role until we were ready to give him one. He was the only present target for our irritation,

so we treated him like extra baggage with which we had been saddled. It was unfair, but I was too distracted by the prospect of the treasures on Laura's thumb drive and the significance of what we were doing to give much more thought to Ewen.

Laura had given me a five-minute tutorial on the secure computer system in the car and said she intended to sleep on the plane. She handed over the thumb drive and suggested that I start looking at her set of documents. Once we arrived in Hong Kong, she said, the source would ensure I had full access to my own complete set.

After the plane took off, I pulled out my new air gapped computer, inserted Laura's thumb drive, and followed her instructions for loading the files.

For the next sixteen hours, despite my exhaustion, I did nothing but read, feverishly taking notes on document after document. Many of the files were as powerful and shocking as that initial PRISM PowerPoint presentation I had seen back in Rio. A lot of them were worse.

One of the first I read was an order from the secret Foreign Intelligence Surveillance Act (FISA) court, which had been created by Congress in 1978, after the Church Committee discovered decades of abusive government eavesdropping. The idea behind its formation was that the government could continue to engage in electronic surveillance, but to prevent similar abuse, it had to obtain permission from the FISA court before doing so. I had never seen a FISA court order before. Almost nobody had. The court is one of the most secretive institutions in the government. All of its rulings are automatically designated top secret, and only a small handful of people are authorized to access its decisions.

The ruling I read on the plane to Hong Kong was amazing for several reasons. It ordered Verizon Business to turn over to the NSA "all call detail records" for "communications (i) between the United States and abroad; and (ii) wholly within the United States, including local telephone calls." That meant the NSA was secretly and indiscriminately collecting the telephone records of tens of millions of Americans, at least. Virtually nobody had any idea that the Obama administration was doing any such thing. Now, with this ruling, I not only knew about it but had the secret court order as proof.

Moreover, the court order specified that the bulk collection of American telephone records was authorized by Section 215 of the Patriot Act. Almost more than the ruling itself, this radical interpretation of the Patriot Act was especially shocking.

What made the Patriot Act so controversial when it was enacted in the wake of the 9/11 attack was that Section 215 lowered the standard the government needed to meet in order to obtain "business records," from "probable cause" to "relevance." This meant that the Federal Bureau of Investigation, in order to obtain highly sensitive and invasive documents—such as medical histories, banking transactions, or phone records—needed to demonstrate only that those documents were "relevant" to a pending investigation.

But nobody—not even the hawkish Republican House members who authored the Patriot Act back in 2001 or the most devoted civil liberties advocates who depicted the bill in the most menacing light—thought that the law empowered the US government to collect records on *everyone*, in bulk and indiscriminately. Yet that's exactly what this secret FISA court order, open on my laptop as I flew to Hong Kong, had concluded when instructing Verizon to turn over to the NSA all phone records for all of its American customers.

For two years Democratic senators Ron Wyden of Oregon and Mark Udall of New Mexico had been going around the country warning that Americans would be "stunned to learn" of the "secret interpretations of law" the Obama administration was using to vest itself with vast, unknown spying powers. But because these spying activities and "secret interpretations" were classified, the two senators, who were members of the Senate Intelligence Committee, had stopped short of disclosing to the public what they found so menacing, despite the legal shield of immunity granted to members of Congress by the Constitution to make such disclosures had they chosen to.

I knew as soon as I saw the FISA court order that this was at least part of the abusive and radical surveillance programs Wyden and Udall had tried to warn the country about. I instantly recognized the order's significance. I could barely wait to publish it, sure that its exposure would trigger an earthquake, and that calls for transparency and accountability

were sure to follow. And this was just one of hundreds of top secret documents I read on my way to Hong Kong.

Yet again, I felt my perspective shift on the significance of the source's actions. This had already happened three times before: when I first saw the emails Laura had received, then again when I began speaking to the source, and yet again when I'd read the two dozen documents he sent by email. Only now did I feel that I was truly beginning to process the true magnitude of the leak.

On several occasions on the flight, Laura came over to the row where I was sitting, which faced the bulkhead of the plane. As soon as I saw her, I would pop up out of my seat and we'd stand in the open space of the bulkhead, speechless, overwhelmed, stunned by what we had.

Laura had been working for years on the subject of NSA surveillance, herself repeatedly subjected to its abuses. I had been writing about the threat posed by unconstrained domestic surveillance going back to 2006, when I published my first book, warning of the lawlessness and radicalism of the NSA. With this work, both of us had struggled against the great wall of secrecy shielding government spying: How do you document the actions of an agency so completely shrouded in multiple layers of official secrecy? At this moment, we had breached that wall. We had in our possession, on the plane, thousands of documents that the government had desperately tried to hide. We had evidence that would indisputably prove all that the government had done to destroy the privacy of Americans and people around the world.

As I continued reading, two things struck me about the archive. The first was how extraordinarily well organized it was. The source had created countless folders and then sub-folders and sub-sub-folders. Every last document had been placed exactly where it belonged. I never found a single misplaced or misfiled document.

I had spent years defending what I view as the heroic acts of Chelsea (then Bradley) Manning, the army private and whistle-blower who became so horrified at the behavior of the US government—its war crimes and other systematic deceit—that she risked her liberty to disclose classified documents to the world through WikiLeaks. But Manning was criticized (unfairly and inaccurately, I believe) for supposedly leaking

documents that she had not first reviewed—in contrast to Daniel Ellsberg, the critics speculated. This argument, baseless though it was (Ellsberg was one of Manning's most devoted defenders, and it seemed clear that Manning had at least surveyed the documents), was frequently used to undermine the notion that Manning's actions were heroic.

It was clear that nothing of the sort could be said about our NSA source. There was no question that he had carefully reviewed every document he had given us, that he had understood their meaning, then meticulously placed each one in an elegantly organized structure.

The other striking facet of the archive was the extent of government lying it revealed, evidence of which the source had prominently flagged. He had titled one of his first folders "BOUNDLESS INFORMANT (NSA lied to Congress)." This folder contained dozens of documents showing elaborate statistics maintained by the NSA on how many calls and emails the agency intercepts. It also contained proof that the NSA had been collecting telephone and email data about millions of Americans every day. BOUNDLESS INFORMANT was the name of the NSA program designed to quantify the agency's daily surveillance activities with mathematical exactitude. One map in the file showed that for a thirty-day period ending in February 2013, one unit of the NSA collected more than *three billion* pieces of communication data from US communication systems alone.

The source had given us clear proof that NSA officials had lied to Congress, directly and repeatedly, about the agency's activities. For years, various senators had asked the NSA for a rough estimate of how many Americans were having their calls and emails intercepted. The officials insisted they were unable to answer because they did not and could not maintain such data: the very data extensively reflected in the "BOUNDLESS INFORMANT" documents.

Even more significant, the files—along with the Verizon document—proved that the Obama administration's senior national security official, Director of National Intelligence James Clapper, lied to Congress when, on March 12, 2013, he was asked by Senator Ron Wyden: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"

Clapper's reply was as succinct as it was dishonest: "No, sir."

In sixteen hours of barely interrupted reading, I managed to get through only a small fraction of the archive. But as the plane landed in Hong Kong, I knew two things for certain. First, the source was highly sophisticated and politically astute, evident in his recognition of the significance of most of the documents. He was also highly rational. The way he chose, analyzed, and described the thousands of documents I now had in my possession proved that. Second, it would be very difficult to deny his status as a classic whistle-blower. If disclosing proof that top-level national security officials lied outright to Congress about domestic spying programs doesn't make one indisputably a whistle-blower, then what does?

I knew that the harder it would be for the government and its allies to demonize the source, the more powerful the effect of the source's disclosures would be. The two most favored lines of whistle-blower demonization—"he's unstable" and "he's naive"—were not going to work here.

Shortly before landing, I read one final file. Although it was entitled "README_FIRST," I saw it for the first time only at the very end of the flight. This document was another explanation from the source for why he had chosen to do what he did and what he expected to happen as a result, and it was similar in tone and content to the manifesto I had shown the *Guardian* editors.

But this document had facts the others did not. It included the source's name—the first time I learned it—along with clear predictions for what would likely be done to him once he identified himself. Referring to events that proceeded from the 2005 NSA scandal, the note ended this way:

> Many will malign me for failing to engage in national relativism, to look away from [my] society's problems toward distant, external evils for which we hold neither authority nor responsibility, but citizenship carries with it a duty to first police one's own government before seeking to correct others. Here, now, at home, we suffer a government that only grudgingly allows limited oversight, and refuses accountability when crimes are committed. When marginalized youths commit minor infractions, we as

a society turn a blind eye as they suffer insufferable consequences in the world's largest prison system, yet when the richest and most powerful telecommunications providers in the country knowingly commit tens of millions of felonies, Congress passes our nation's first law providing their elite friends with full retroactive immunity—civil and criminal—for crimes that would have merited the longest sentences in [] history.

These companies . . . have the best lawyers in the country on their staff and they do not suffer even the slightest consequences. When officials at the highest levels of power, to specifically include the Vice President, are found on investigation to have personally directed such a criminal enterprise, what should happen? If you believe that investigation should be stopped, its results classified above-top-secret in a special "Exceptionally Controlled Information" compartment called STLW (STELLARWIND), any future investigations ruled out on the principle that holding those who abuse power to account is against the national interest, that we must "look forward, not backward," and rather than closing the illegal program you would expand it with even more authorities, you will be welcome in the halls of America's power, for that is what came to be, and I am releasing the documents that prove it.

I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end. I will be satisfied if the federation of secret law, unequal pardon, and irresistible executive powers that rule the world that I love are revealed for even an instant. If you seek to help, join the open source community and fight to keep the spirit of the press alive and the internet free. I have been to the darkest corners of government, and what they fear is light.

Edward Joseph Snowden, SSN: [redacted]

CIA Alias "[redacted]"

Agency Identification Number: [redacted]

Former Senior Advisor | United States National Security Agency, under corporate cover

Former Field Officer | United States Central Intelligence Agency, under diplomatic cover

Former Lecturer | United States Defense Intelligence Agency, under corporate cover

Buy the Book:

amazon.com BARNES&NOBLE INDIEBOUND macmillan

E-BOOK

amazonkindle iBooks kobo nook