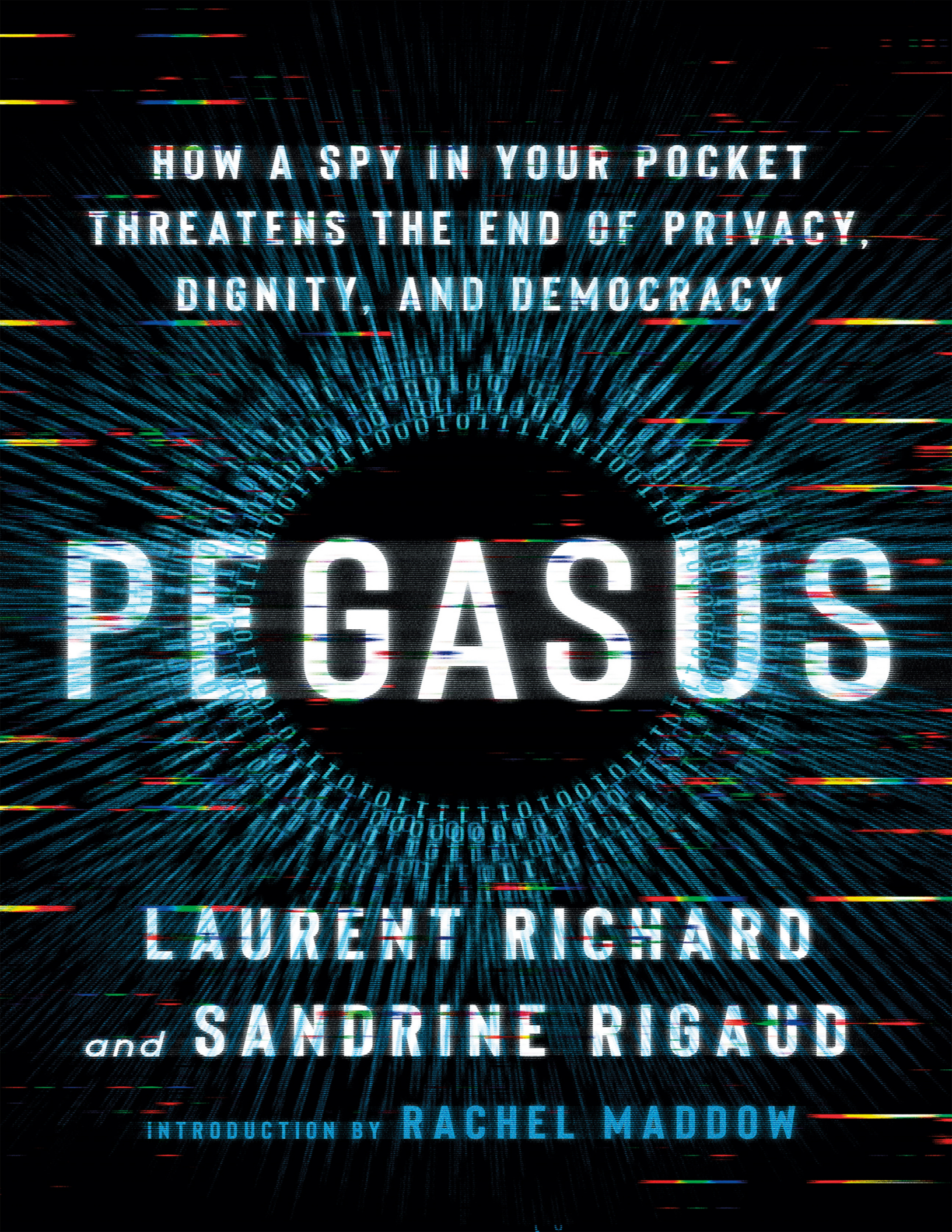
HOW A SPY IN YOUR POCKET THREATENS THE END OF PRIVACY, DIGNITY, AND DEMOCRACY
PEGASUS
LAURENT RICHARD
and SANDRINE RIGAUD
INTRODUCTION BY RACHEL MADDOW

PEGASUS

HOW A SPY IN YOUR POCKET THREATENS THE END OF PRIVACY, DIGNITY, AND DEMOCRACY

LAURENT RICHARD AND
SANDRINE RIGAUD

HENRY HOLT AND COMPANY
NEW YORK

INTRODUCTION

Rachel Maddow

The call appeared urgent, in that it was coming at close to midnight Tel Aviv time, August 5, 2020, from somebody in senior management at the NSO Group. Cherie Blair, former First Lady of the United Kingdom, longtime barrister, noted advocate for women entrepreneurs in Africa, South Asia, and the Middle East, a prominent voice for human rights worldwide, was obliged to pick up the phone. Mrs. Blair had recently signed on as a paid consultant to the Israeli firm NSO to help "incorporate human rights considerations into NSO activities, including interactions with customers and deployment of NSO products."

This was a delicate high-wire act, ethically speaking, because NSO's signature product, cybersurveillance software called Pegasus, was a remarkable and remarkably unregulated tool—extraordinarily lucrative to the company (NSO grossed around $250 million that year) and dangerously seductive to its clients. Successfully deployed, Pegasus essentially owns a mobile phone; it can break down defenses built into a cell phone, including encryption, and gain something close to free rein on the device, without ever tipping off the owner to its presence. That includes all text and voice communications to and from the phone, location data, photos and videos, notes, browsing history, even turning on the camera and the microphone of the device while the user has no idea it's happening. Complete remote personal surveillance, at the push of a button.

NSO insists its software and support services are licensed to sovereign states only, to be used for law enforcement and intelligence purposes. They insist that's true, because—my God—imagine if it weren't.

The cybersurveillance system the company created and continually updates and upgrades for its sixty-plus clients in more than forty different countries has made the world a much safer place, says NSO. Tens of thousands of lives have been saved, they say, because terrorists, criminals, and pedophiles (pedophiles

is a big company talking point the last few years) can be spied on and stopped before they act. The numbers are impossible to verify, but the way NSO describes it, the upsides of Pegasus, used within legal and ethical boundaries, are pretty much inarguable. Who doesn't want to stop pedophiles? Or terrorists? Who could be against it?

"Mission Control, we have a problem," was the message Cherie Blair got from the call that warm summer evening in August 2020.

"It had come to the attention of NSO that their software may have been misused to monitor the mobile phone of Baroness Shackleton and her client, Her Royal Highness Princess Haya," Blair explained in a London court proceeding some months later. "The NSO Senior Manager told me that NSO were very concerned about this."

NSO's concern appeared to be twofold, according to the evidence elicited in that London court. The first was a question of profile. Pegasus had been deployed against a woman who was a member of *two* powerful Middle Eastern royal families, as well as her very well-connected British attorney, Baroness Fiona Shackleton. Shackleton was not only a renowned divorce lawyer to the rich and famous—including Paul McCartney, Madonna, Prince Andrew, and Prince Charles—she was also herself a member of the House of Lords. Even more problematic for NSO, it was an outside cybersecurity researcher who had discovered the attacks on the baroness and the princess. If he'd figured out this one piece of how Pegasus was being used, what else had he figured out? And how much of this was about to become public knowledge?

The caller from NSO asked Cherie Blair "to contact Baroness Shackleton urgently so that she could notify Princess Haya," she explained in testimony. "The NSO Senior Manager told me that they had taken steps to ensure that the phones could not be accessed again."

The details of the late-night call to Blair and the spying on the princess and her lawyer didn't really shake out into public view until more than a year later, and only then because it was part of the child custody proceedings between Princess Haya and her husband, Sheikh Mohammed bin Rashid Al Maktoum, prime minister of the United Arab Emirates and the emir of Dubai. The finding by the president of the High Court of Justice Family Division, released to the public in October 2021, held that the mobile phones of the princess, her lawyer, the baroness, and four other people in their intimate circle were attacked with cybersurveillance software, and that "the software used was NSO's Pegasus." The judge determined it was more than probable that the surveillance "was

carried out by servants or agents of [the princess's husband, Sheikh Mohammed bin Rashid Al Maktoum], the Emirate of Dubai, or the UAE." The surveillance, according to the judge, "occurred with [the Sheikh's] express or implied authority."

The story of the princess, the baroness, and Pegasus might have faded into gossip columns and then into oblivion after a few weeks. A rich and powerful man used a pricey bit of software to spy on his wife and her divorce lawyer? Well, if you marry a sheikh and then cross him, you damn well might expect things to get weird. NSO also did a fairly nice job of cleanup on Aisle Spyware. The court finding pretty much accepted the word of NSO that it had terminated the UAE's ability to use its Pegasus system altogether, at a cost to the company, the judge noted, "measured in tens of millions of dollars." And maybe they did, but who can say.

A FUNNY THING happened on the way to that divorce court gossip column item, though. Because right around the time Cherie Blair got that call from Israel, a very brave source offered two journalists from Paris and two cybersecurity researchers from Berlin access to a remarkable piece of leaked data. The list included the phone numbers of not one or two or ten Emirati soon-to-be divorcees, or even twenty or fifty suspected pedophiles or drug traffickers. It was fifty *thousand* mobile phone numbers, all selected for possible Pegasus targeting by clients of that firm in Israel, NSO. Fifty thousand?

What exactly to make of that initial leaked list—that crucial first peek into the abyss—is a question that took nearly a year to answer, with a lot of risk and a lot of serious legwork to get there. The answer to the question matters. Because either this is a scandal we understand and get ahold of and come up with solutions for, or this is the future, for all of us, with no holds barred.

THIS BOOK IS the behind-the-scenes story of the Pegasus Project, the investigation into the meaning of the leaked data, as told by Laurent Richard and Sandrine Rigaud of Forbidden Stories, the two journalists who got access to the list of fifty thousand phones. With the list in hand, they gathered and coordinated an international collaboration of more than eighty investigative journalists from seventeen media organizations across four continents, eleven time zones, and about eight separate languages. "They held this thing together

miraculously," says an editor from the *Guardian*, one of the partners in the Pegasus Project. "We've got, like, maybe six hundred journalists. The *Washington Post* is maybe twice the size. And to think that a small nonprofit in Paris, with just a handful of people working for it, managed to convene a global alliance of media organizations and take on not just one of the most powerful cybersurveillance companies in the world but some of the most repressive and authoritarian governments in the world, that is impressive."

In the daily back-and-forth of American news and politics—my wheelhouse—it is rare indeed to come across a news story that is both a thriller and of real catastrophic importance. Regular civilians being targeted with military-grade surveillance weapons—against their will, against their knowledge, and with no recourse—is a dystopian future we really are careening toward if we don't understand this threat and move to stop it. The Pegasus Project saga not only shows us how to stop it; it's an edge-of-your-seat procedural about the heroes who found this dragon and then set out to slay it. I have never covered a story quite like this, but Laurent and Sandrine sure have, and it is freaking compelling stuff.

The engine of the narrative you're about to read is the risky investigation itself, from the minute these guys first got access to that leaked list in the last half of 2020 to publication in July 2021. But herein also is the story of the company NSO, its Israeli government benefactors, and its client states, which takes the reader from Tel Aviv to Mexico City to Milan, Istanbul, Baku, Riyadh, Rabat, and beyond. The company's ten-year rise—from its unlikely inception, to its early fights with competitors, to its golden era of reach and profitability—reveals the full history of the development, the weaponization, and the mindless spread of a dangerous and insidious technology. "If you're selling weapons, you better make sure you're selling those to someone who is accountable for their actions," one young Israeli cybersecurity expert says. "If you're giving a police officer a gun and if that police officer starts shooting innocent people, you are not to be blamed. But if you're giving a chimpanzee a gun and the chimpanzee shoots someone, you can't blame the chimpanzee. Right? You will be to blame." Turns out this story has armed chimpanzees up the wazoo. And a lot of innocent people shot at by the proverbial police, too.

Here also is the story of the other individuals besides Laurent and Sandrine who were entrusted with full access to the leaked data, Claudio Guarnieri and Donncha Ó Cearbhaill (pronounced O'Carroll), two young, incorrigible, irrepressible cybersecurity specialists at Amnesty International's Security Lab.

These men—one barely in his thirties, the other still in his twenties—shouldered incredible weight throughout the Pegasus Project. Against the most aggressive and accomplished cyberintrusion specialists in the world, Claudio and Donncha were charged with designing and enforcing the security protocols that kept the investigation under wraps for almost a full year and kept the source that provided the list out of harm's way for good.

More than that, it was up to Claudio and Donncha to find the evidence of NSO's spyware on phones that were on the list leaked to them by that brave source. The insidious power of a Pegasus infection was that it was completely invisible to the victim—you'd have no way to know the baddies were reading your texts and emails and listening in on your calls and even your in-person meetings until they used their ability to track your exact location to send the men with guns to meet you. For the Pegasus Project to succeed in exposing the scale of the scandal, the journalists knew they would need to be able to diagnose an infection or an attempted infection on an individual phone. Claudio and Donncha figured out how to do it. Working quite literally alone, these two took on a multibillion-dollar corporation that employed 550 well-paid cyberspecialists, many with the highest levels of military cyberwarfare training. To best that Goliath, these two Davids had to fashion their own slingshot, had to invent the methods and tools of their forensics on the fly. That they succeeded is as improbable as it is important, for all our sakes.

Here also is the story of the victims of Pegasus. Among them are those who hold enough power that you might expect they'd be protected from this kind of totalist intrusion—heads of state, high-ranking royals, senior politicians, law enforcement figures. And then there's the people whom governments the world over have always liked to put in the crosshairs: opposition figures, dissidents, human rights activists, academics. Laurent and Sandrine rack focus tight on the group most represented in the leaked data, of course: journalists.

For me, the most unforgettable characters in this story are Khadija Ismayilova, from Azerbaijan, and Omar Radi, of Morocco. Their uncommon courage proves both admirable and costly. Their stories lay bare the awful personal consequences of challenging governments in an age of unregulated cybersurveillance, and the need for more people like them.

As antidemocratic and authoritarian winds gather force all over the world, it's increasingly clear that the rule of law is only so powerful against forces hell-bent on eliminating the rule of law. If we've learned anything over the last five years, it's this: there will be no prosecutor on a white horse, no flawless

court proceedings where a St. Peter in black robes opens or closes the pearly gates based on true and perfect knowledge of the sins of those in the dock. Sometimes, sure, the law is able to help. But more often, the threat evades, outmaneuvers, or just runs ahead of the law in a way that leaves us needing a different kind of protection. Again and again, it falls to journalists to lay out the facts of corruption, venality, nepotism, lawlessness, and brutality practiced by the powerful.

The dangers of doing this kind of work are real, and growing. For all the prime ministers and royal soon-to-be-ex-wives and other high-profile targets that NSO clients hit, it is no surprise that Pegasus has been turned full blast on reporters and editors in order to harass, intimidate, and silence. If this antidemocratic, authoritarian nightmare can't be safely reported upon, it won't be understood. And if it isn't understood, there's no chance that it will be stopped.

WHERE'S YOUR PHONE right now? That little device in your pocket likely operates as your personal calendar, your map and atlas, your post office, your telephone, your scratchpad, your camera—basically as your trusted confidant. Matthew Noah Smith, a professor of moral and political philosophy, wrote in 2016 that a mobile phone "is an extension of the mind.… There is simply no principled distinction between the processes occurring in the meaty glob in your cranium and the processes occurring in the little silicon, metal, and glass block that is your iPhone. The solid-state drive storing photos in the phone are your memories in the same way that certain groups of neurons storing images in your brain are memories. Our minds extend beyond our heads and into our phones."

Professor Smith was making the case back then for a zone of privacy that extended to our mobile phone. If the state has no right to access the thoughts in our head, why should it have the right to access the pieces of our thoughts that we keep in our mobile phone? We tell our cell phones almost anything these days, even things we aren't cognizant of telling it, and use it as the conduit to offer the most intimate glimpses of ourselves. (See sexting.) If you believe your privacy is being secured by encryption, please read this book, and consider the fifty thousand people on that horror show list, who unbeknownst to them were targeted to unwillingly share every single thing that passed through their phones with people who only had to pay for the privilege.

That list of fifty thousand was just our first keyhole view of the crime scene. If they could do it for fifty thousand, doesn't that mean they could do it for five hundred thousand? Five million? Fifty million? Where is the limit, and who is going to draw that line? Who is going to deliver us from this worldwide Orwellian nightmare? Because it turns out you don't have to be married to the emir of anything to find your every thought, every footstep, every word recorded and tracked from afar. Turns out you just need to have a phone, and a powerful enemy somewhere. Who among us is exempt from those conditions?

Where did you say your phone is right now?

CHAPTER ONE

THE LIST

Laurent

Sandrine and I had been drawn to Berlin by the kind of opportunity you get maybe once in a lifetime in journalism—a shot to break a story that could have serious implications around the world. It felt kind of fitting that our taxi from the airport to the city center skirted within a few kilometers of the Stasi Museum, a complex that once housed the apparatus of the East German secret police, "The Sword and Shield of the State." This investigation, if we decided to undertake it, would have to contend with swords and shields wielded by a dozen or more very defensive state actors and by a billion-dollar private technology corporation operating under the protection of its own very powerful national government.

The taxi ride was the last leg of a trip that seemed to portend a rise of obstacles. The limitations put in place during the latest wave of Covid-19 had laid waste to familiar routines. The simple two-hour trip from Paris to Berlin had taken triple that, and included a connection through the food desert of an airport in Frankfurt, and the indignity of German soldiers shoving cotton swabs up our nasal cavities before we were allowed to exit the airport in Berlin.

By the time Sandrine and I stumbled into our sleekly modern and well-lighted little rented flat above Danziger Strasse, we were both so knackered that dark-of-the-night questions were already preying on us. Was this really the best time to dive into another difficult and all-consuming investigation? Our nine-person team at Forbidden Stories was deep into its third major project in just three years; the current investigation, the Cartel Project, was already shaping up as the most dangerous we had done to date. And we still had a lot of work to do to be ready for publication. We were developing leads on the most murderous drug gangs in Veracruz and Sinaloa and Guerrero, on the chemicals needed to

produce the supercharged opioid fentanyl, which were being trafficked into the country from Asia, and on the lucrative gun trade filling the cartels' private armories (as well as the bank accounts of gun manufacturers and private gunrunners in Europe, Israel, and the United States).

We were essentially picking up reporting threads left unfinished by a handful of brave Mexican journalists who had been killed, most likely by assassins from the local drug cartels whose violent and criminal activities the reporters had been investigating. Outside of active war zones, Mexico was and remains to this day the most dangerous place in the world to be a journalist committed to telling the truth about bad guys. More than 120 journalists and media staffers had been killed in Mexico in the first two decades of the twenty-first century. Another score or so had simply disappeared without a trace.

This meant the Cartel Project tied seamlessly to the mission of Forbidden Stories: we aim to put bad actors and repugnant governments on notice that killing the messenger will not kill the message. Which means collaboration is an indispensable tool. There is strength and safety in numbers. The more journalists who are working the story, the more certain it is to see print. We had begun inviting into the Cartel Project reporters from our trusted media partners, including *Le Monde* in Paris, the *Guardian* in London, and *Die Zeit* and *Süddeutsche Zeitung* in Germany. The team would eventually grow to more than sixty reporters from twenty-five different media outlets in eighteen countries. But the beating heart of the project, already, was Jorge Carrasco, who was the director of the most intrepid investigative publication in Mexico, the weekly magazine *Proceso.* A stubborn and celebrated reporter himself, Jorge was also a colleague, and an exact contemporary of the woman who was emerging as a figure at the center of our investigation, Regina Martínez.

Carrasco was still a reporter at *Proceso* in April 2012 when the news reached him that his co-worker had been beaten and strangled to death in her home. Regina had been a journalist for nearly a quarter century by then and had spent much of the previous four years dogging the powerful and dangerous drug cartel that had essentially taken over Veracruz. Cash was flowing into the region, along with waves of violence that convulsed the state's teeming port city and spread into the surrounding area. A large portion of Martínez's final reporting was in uncovering the destabilizing relationships growing up between local politicians, local law enforcement, and local drug lords. She hadn't really gone looking for the story, but if you were a sentient being in Veracruz in those years, it was hard to miss. And once she was on it, Regina had a hard time

backing off even after she knew she was on perilous ground. She had confided to her closest friends, just a few months before her death, that she might have gone too far, and she feared for her safety. She was worried enough to stop using a byline on the most incendiary of her stories, but she refused to quit reporting.

A few weeks before she was found strangled to death, Regina had published a damning report detailing the personal assets amassed by two public officials who had allied themselves with the Los Zetas cartel in Veracruz. (Three thousand copies of that issue of *Proceso* were removed from the kiosk shelves before they ever made it into the hands of local readers.) At the time of her murder, she was in the middle of investigating the story of the thousands of people who had mysteriously disappeared from Veracruz in the previous few months. "Her death marked a before and after for the profession," one of Martínez's friends and colleagues would tell us. "She was part of a major national magazine. We thought she was protected."

Jorge had already traveled to our offices in Paris to brief the Forbidden Stories team and our early partners on the state of investigative reporting in Mexico and the outlines of the Regina Martínez story. The fifty-six-year-old journalist spoke with a soft, measured cadence befitting a classics scholar, but his message to us was sharp and compelling. "Regina's murder was a point of no return," Jorge had explained. "A very clear message that the [cartels] could continue to kill journalists and nothing happens."

The police and prosecutors in Veracruz, Jorge told us, basically punted Regina's case in 2012, pinning her murder on a low-rent criminal who quickly recanted his confession (which the suspect claimed he made only after hours of physical torture by local police). For most of the eight years since, Jorge had been determined to get to the bottom of Regina's killing. He had taken to heart the admonition of Julio Scherer García, the founding editor of *Proceso* and the godfather of investigative journalism in Mexico. "The world has hardened, and I think journalism will have to harden," Scherer said not long before he died in 2015. "If the rivers turn red and the valleys fill with corpses … journalism will have to tell that story with images and words. Heavy tasks await us."

Jorge Carrasco worked the story for years in spite of threats and intimidation, and even after the murder of a second *Proceso* contributor, who also demanded answers from the government about Martínez, but with little success. By January 2020, when Sandrine and I first visited the Mexico City offices of *Proceso*—offices with a security protocol you might expect at a

bunkered police station, with a guard at the front gate and bars on every window—Jorge's ardor had cooled. He admitted to us that they had discussed it in the newsroom, as a staff, and decided chasing the truth about Regina Martínez's murder was too dangerous. If they kept it up, others were likely to die at the hands of the local drug lords.

Once he learned an international consortium of journalists was willing to take up the story, though, Jorge seemed reenergized. He had dispatched his chief archivist to dig up all of Regina's stories from *Proceso* in the years before her death, and he asked us to loop another of his reporters into the top-secret Signal group used by key members of the Cartel Project. But the last Sandrine had heard from Jorge on the Signal app, not long before our trip to Berlin, he had sounded a little shaky—lamenting the ongoing damage done by Covid-19 to his magazine's already slim and always wobbly profit margin. "I'm okay but worried," he wrote. "Sales of *Proceso* are really falling."

★ ★ ★

I WAS KEYED up when the buzzer to our East Berlin flat rang the next morning. We hadn't yet mastered the electronic entry system to our short-term rental, so I raced down the stairs and opened the front door for our two guests. The first I saw was a pale, wraithlike, thirtysomething man with wire-rim glasses and a ski cap pulled tight atop his skull. He looked like the kind of guy who spent a lot of time indoors at a computer screen. I welcomed him with a cheery hello and stuck my hand out in greeting. Claudio Guarnieri, senior technologist at Amnesty International's Security Lab, didn't offer any pleasantries in response, didn't shake my hand, didn't even really pause long enough to make eye contact. He simply bade me to direct him and the skinny young fellow with him up the stairs and into our flat, where we could get down to business at the dining room table.

But there would be *no* business, Claudio explained, until we all powered down our phones and our laptops, put them in the next room, and closed the door on them. The cloak-and-dagger aspect of these instructions was not entirely unexpected, given the reason for this meeting, but I was surprised by Claudio's brusque tone. He was polite enough, but not long on social niceties; in fact, he didn't seem to be much concerned whether we liked him or not. This was an *alliance de circonstance*, after all, and compatibility mattered a lot less than viability.

We hastily stowed our electronic devices in the next room, but not before I took note of the sticker on Claudio's own laptop, a quote from the Mexican political dissident Subcomandante Marcos: "We are sorry for the inconvenience, but this is a revolution." Back at the table, Claudio waved away any attempt at small talk and turned immediately to the reason we were all there. We had been chosen—Forbidden Stories and Amnesty International's Security Lab—as the only two groups with access to a document we had taken to calling the List. Sandrine and I had each been given to understand that the data might help us uncover the existence of a system of truly insidious surveillance, made possible by a private for-profit corporation, that touched thousands of unsuspecting individuals on almost every continent.

We were a long way from proving that, we all knew, at our table in Berlin that morning. The data in this list was a bit of a cipher: a scroll of tens of thousands of phone numbers from all over the world, as well as some time stamps. Only a handful of those numbers had been matched to actual names or identities. What we did know was that each number represented a person whose cell phone had been selected for potential infection with the most potent cybersurveillance weapon on the market: a malware called Pegasus, which had been developed, marketed, and supplied to law enforcement and national security agencies in more than forty countries around the world by the alpha dog in the burgeoning industry—the Israeli tech company NSO.

Pegasus was coveted by national security specialists around the globe because it was regarded as state-of-the-art spyware; if a country wanted to catch the bad guys in criminal or terrorist acts, or to prevent those acts before they happened, Pegasus was a godsend. Each successful infection allowed its operator, or end user, to essentially take over a cell phone. Law enforcement or national security agencies would have access to every jot and tittle in that phone, *before* any outgoing communication was encrypted and *after* any incoming communication was decrypted. The operators of Pegasus could track that cell phone's geolocation and exfiltrate email messages, text messages, data, photographs, and videos. Pegasus also allowed its users to gain control of the device's microphones and cameras; these recording apps could be turned on remotely, at will, at the pleasure and convenience of the end user.

The dangerous hitch in the Pegasus system was that it had not been limited to spying on bad guys. By the time we sat down in Berlin with Claudio and his number two, Donncha Ó Cearbhaill, a few dozen cases of misuse had already been documented. Cybersecurity experts at the University of Toronto's Citizen

Lab and at Claudio's Amnesty International's Security Lab had found cases of Pegasus being used to target human rights defenders, lawyers, and journalists. The specialists in those forensic labs had not only elucidated many of the mechanics and capabilities of Pegasus but had called out some of its most pernicious end users. WhatsApp had filed suit against NSO, claiming fourteen hundred of its users had been surreptitiously targeted by Pegasus in just one two-week period. Amnesty International had a pending suit also. The public domain was filling with information gleaned from legal filings in courts from the United States to France to Israel to Canada.

There had also been some really good journalism and a growing body of scholarship on the rise of the for-profit "Intrusion as a Service" industry in general and NSO in particular. These multiple investigations, taken together, were starting to look like a more successful edition of the Blind Men and the Elephant parable. The combination of cybersecurity experts, academics, journalists, and justice-seeking victims, working separately and in concert, had managed to sketch a pretty complete picture of the cybersurveillance elephant at work.

The outlines alone made crystal clear the threats to human rights and privacy, and yet, even the most dismaying headlines and the most granular forensic analyses had had little to no real impact. Outside of calls from Amnesty International and Citizen Lab and the United Nations special rapporteur on the promotion and protection of the right to freedom of opinion and expression, there was virtually no public outcry and very little actual attention. No governing body of consequence was putting any fetters on the industry. NSO's profits and its client base were growing faster than ever, with customers across Europe, North America, the Middle East, and Africa. "The few of us invested in these issues warned again and again how the commodification of surveillance was paving the way to systemic abuse," Claudio would later say, reflecting on a decade's worth of consistent effort and consistent frustration. "Very few listened; most were just indifferent. Every new report, every new case, felt so inconsequential that I started questioning whether insisting on them was serving anything other than our own egos."

That's what made this leak so enticing.

Claudio never grew particularly animated our first day together in Berlin, or any other day thereafter. He was always careful not to betray any outward sense of excitement. But he clearly held hope that this leaked list might finally help him get the goods on NSO and allow us to draw the sort of public attention this

unfolding crisis truly deserved. Claudio and Donncha were slightly ahead of us in their understanding of the list itself, partly because of the technical skills they had developed over the last decade and partly because the Security Lab had access to digital tools that Forbidden Stories lacked. Claudio set the agenda for much of that first day at that dining room table in Berlin, sitting on a sleek wooden bench, explaining the big picture of this story as he apprehended it at that moment.

Time stamps in the data went back almost five years and extended right up to the past few weeks, Claudio explained, which meant the attacks were fresh—and possibly even ongoing. We were likely to be investigating a crime in progress. He and Donncha had already started the laborious process of identifying exactly who was attempting to spy on whom. And exactly when. And exactly where. The list of phone numbers was arranged in clusters, suggesting which of NSO's many client countries was targeting any specific individual. The governments selecting targets ranged from murderous dictatorships to would-be autocracies to the largest democracy on the planet. The most active client state by far was Mexico, with more than fifteen thousand separate numbers selected for possible targeting.

The list no doubt contained hundreds of cell phone numbers of authentic drug lords, terrorists, criminals, and national security threats—the sort of malefactors NSO spokespeople claimed Pegasus was designed to thwart. But what Claudio and Donncha had already learned about the range of targets selected for attack was eye-popping. When the two had started the process of identifying some of the phone numbers on the list, Claudio explained to us, it turned out that many belonged to academics, human rights defenders, political dissidents, government officials, diplomats, businessmen, and high-ranking military officers. Claudio and Donncha had already found hundreds of noncriminal, non-terrorist targets selected for possible Pegasus infection, and they had barely scratched the surface. The group with the largest number of targets on its collective back—well over 120 and counting—was journalists.

If the data in this list led us to the hard evidence necessary for publication, we all understood, we would not only be able to reconfirm the already-known fact that cyberintrusion and cybersurveillance were being weaponized to stifle the free press and to undermine and intimidate political dissent. We would be able to reveal that it was being weaponized at a sweep and scale that astounds—and horrifies.

As Claudio, Donncha, Sandrine, and I scrolled down through page after page after page of possibly compromised cell phone numbers, it occurred to me that we were not merely groping around to help define the outlines of a single rogue elephant. We were looking at a herd of hundreds, thousands, maybe even tens of thousands of elephants thundering unimpeded across the plains, prodded by some of the most vicious political regimes on the planet, and headed right for cherished and necessary pillars of civil society. The large-scale, unchecked, systematic abuse of cybersurveillance weapons was a clear and present danger to the most basic human rights, including privacy, political dissent, freedom of expression, and freedom of the press; it was a threat to democracy itself, at a time when the world's most stable democracies were under relentless attack from without and from within.

★ ★ ★

THE FIRST LOOK at the list was slightly disorienting. The pull was magnetic, almost like a physical sensation. I reminded myself to take a deep breath occasionally, as Claudio kept talking, noting, for instance, that it looked like Moroccan intelligence had targeted an extraordinary number of French cell phones. I had to tell myself not to let my imagination get too far ahead of me. Skepticism is crucial for any reporter—a stopgap to embarrassing mistakes, like being played by an unscrupulous source with an axe to grind, or letting excitement about a potentially big story outrun good sense and rigorous vetting. Vetting the data in this list would take months. Finding victims who were willing to allow us to analyze their phones for evidence of Pegasus targeting (and to keep quiet about it while we developed the story) would be a delicate operation. Claudio and Donncha faced a more daunting task, even with potentially compromised phones in hand to analyze. NSO had designed Pegasus as more than a Trojan horse; it was engineered to be an *invisible* Trojan horse. Top-shelf cybersurveillance exploits aim to leave behind no detectable traces, and NSO was believed to be the best in the business at covering its tracks. Gathering unassailable forensic evidence was going to be an uphill battle, and forensics was only half the battle.

Claudio, Donncha, Sandrine, and I were talking about embarking on an investigation of a private company whose entire reason for being is digital surveillance, a company that trumpeted its ability to "Find anyone, anywhere." Considering that foreign governments on five continents had been paying NSO

as much as a quarter of a billion dollars a year to do just that, the company's spyware system was probably very good at it. The four of us understood what we would be stepping into by the time our first meeting came to a close, Claudio most of all. He issued Sandrine and me another brusque set of instructions before we parted: he told us we needed to go out and buy new devices—no SIM cards!—dedicated solely to communicating with one another. There would be no cell phone calls among the four of us or anybody else who came onto the project. No iMessages, no Signal messages, no WhatsApp calls. We had already, at Claudio's insistence, bought new dedicated laptops—PCs, not Macs—so that we could keep a hard wall between the Pegasus Project and all the other work we were doing. If we went ahead with this project, it occurred to me, the main driver of the operation would be paranoia.

When Claudio and Donncha left that evening, after we set a time to meet again the next day, the difficulties of tackling this investigation were already spinning in my head. The list itself was a big unknown. We had plenty of faith in the source of the leak, but that was beside the point. We were looking at months of authenticating the data on the list, double-checking every fact and story that hove up out of those tens of thousands of phone numbers. We were going to have to do this work while attempting to live within the physical and social restrictions imposed on us by the most lethal global heath pandemic in a century. I was also having a hard time imagining forming a comfortable working relationship with Claudio, who had not shown even a hint of a smile that first day. Donncha was much more open and easygoing, but the twenty-seven-year-old cyber-researcher, as we later learned, also had good reason to be wary of reporters. Add to that, this investigation would have to be done within a bubble of absolute secrecy—a bubble easily popped by a single careless mistake.

★ ★ ★

CLAUDIO SUGGESTED AN interesting exercise for our second-day meeting in Berlin, a whack at low-hanging fruit. He pulled from his bag an unused USB stick, still in its packaging, and helped me to safely download a backup of the entirety of my digital contacts file from my personal cell phone. Then Claudio plugged the untainted USB stick into the secure laptop computer he was using to access the list, and ran an automated program that matched cell phone numbers from my contacts file with cell phone numbers in the data. The first to

come up a match was for an official in Turkey's foreign ministry. I had his number because I had requested an interview with him while working on a story about secret arms transfers between the Turkish secret service and jihadist groups in northern Syria.

The next match to come up was the phone number of Khadija Ismayilova, who was the most famous and fearless investigative reporter in Azerbaijan. I knew her well. Khadija had been reporting on the financial corruption of Azeri president Ilham Aliyev for more than fifteen years. The forty-four-year-old Ismayilova had won multiple international press awards for her journalism. She had also earned the wrath of Aliyev and his secret police. Khadija had been harassed, blackmailed, and imprisoned by the Aliyev government; she was at that precise moment living under house arrest in Baku. She had been under almost constant physical surveillance for years.

I had actually seen some of the spooks on Khadija watch—beefy guys with bushy mustaches and ill-fitting trench coats—when I was on a reporting trip in Azerbaijan back in 2014. I was on the lookout for them because the first thing Khadija did when we met was alert me to Aliyev's iron dome of surveillance. Anybody who had been seen in her company, Khadija explained, would likely be spied on. "Don't do anything in your hotel room you wouldn't want to see published," she told me. She wasn't joking.

I had two separate numbers for Khadija, but I had always been careful to only call or text her special secret number, the one I identified as "Khadija-Safe" in my contacts file. Turns out that the number in the leaked data, the number selected for targeting by the Azeri government, was "Khadija-Safe." The possibility that Khadija was still under surveillance was no real surprise. The possibility that she was being stalked by Pegasus was.

NSO was reported to have licensed its spyware system to more than forty countries, but Azerbaijan had never been on anybody's list. If NSO had sold licenses to cybersurveillance weapons to government agencies in Azerbaijan—a country whose annual record of civil liberties violations, political repression, and outright torture put it consistently near the top ten of bad actors alongside China, North Korea, Somalia, and Syria—there was no telling how far and wide Pegasus had flown. That was a chilling thought, because in the short history of the cyberweapons-for-sale industry, surveillance was only the beginning of the problem. Where cybersurveillance was in wide use, serious casualties often followed.

I had first become aware of this industry back in the summer of 2011, when two *Wall Street Journal* reporters had stumbled into a warren of computers in Tripoli a week after rebels had deposed the murderous Libyan dictator Muammar Gadhafi. The office turned out to be the hub of a massive cybermonitoring program. "The recently abandoned room," the *Journal* reporters wrote in their initial story, "is lined with posters and English-language training manuals stamped with the name Amesys, a unit of French technology firm Bull SA, which installed the monitoring center."

Turns out the French company (with the blessing of the French government) had sold Gadhafi an internet surveillance system that allowed his agents to monitor the emails, chats, and messages of anybody in Libya. The Gadhafi regime was able to identify and track the dictator's many political opponents almost at will. "Whereas many Internet interception systems carry out basic filtering on IP addresses and extract only those communications from the global flow (Lawful Interception)," read an Amesys-produced poster hanging in the office in Tripoli, "EAGLE Interception system analyzes and stores all the communications from the monitored link (Massive Interception)."

Libyan security tactics didn't stop at surveillance. Being caught entering a chat room filled with critics of Gadhafi could have serious consequences—starting with arrest and questioning. According to the testimony of several detainees in a French court in 2013, Gadhafi's interrogators were able to quote back to them—verbatim—their emails, SMS exchanges, Facebook threads, chat-room conversations, even private phone conversations. The security agents usually demanded from their captives the identities behind the various user names they had been communicating with online or on the phone. If threats, beatings, electric shock, and other torture weren't enough to convince the detainees to reveal the names of otherwise anonymous comrades, Gadhafi's agents would ship them off to prison. Threats and beatings continued there, along with brief field trips to a courtyard to witness the executions of other prisoners.

When these revelations started to come out in France, Bull SA made the prudent business move. They simply off-loaded the technology that ran the Eagle system to another French company, Nexa Technologies—which continued to make it available on the open market. Egyptian president Abdel Fattah al-Sisi, who seized power following the chaos of the Arab Spring, became one of the French cyberweapon's most enthusiastic end users. (The surveillance system was reported to be a $12 million gift from al-Sisi's friends

in the United Arab Emirates.) “The grave human rights violations committed to this day by the various branches of the [Egyptian] security services include arbitrary mass arrests, with the incarceration of at least 60,000 political prisoners since 2013; extrajudicial executions; enforced disappearances … and the systematic use of torture,” the Paris-based International Federation for Human Rights had noted in a recent report, *Egypt: A Repression Made in France*. “This modus operandi of the security forces, aimed at eliminating all possibility of dissent, has become everyday reality for all Egyptians, and it specifically targets political opponents and civil society: members of political parties, the Muslim Brotherhood and their supporters, activists in revolutionary movements and of all stripes, human rights defenders, lawyers, journalists, writers, researchers, in addition to LGBTQ people or those perceived as such.”

The Bull/Amesys/Nexa axis was hardly alone in selling spyware systems to questionable regimes—regimes that had nevertheless been designated by France as “a bulwark against Islamic fundamentalism,” according to the report. “The enormous increase of arms sales beginning in 2013 and al-Sisi’s arrival in power in Egypt in 2014 have proven profitable for at least eight French companies that have sold equipment—both conventional weapons and surveillance equipment—to Egypt.”

By 2020, cybersurveillance weapons had become an international growth sector, with dozens of countries engaging in active cybersurveillance measures, almost all of them customers of private corporations who were happy to tailor the systems to their clients’ needs and wants. So long as the price was right.

The leading spyware technology companies had, by 2020, adjusted their focus from personal computers to cell phones, with NSO Group right out front. The consequences had been predictable. Security researchers first found evidence of a cell phone infected with NSO’s Pegasus in 2016—in an iPhone owned by a human rights activist in the United Arab Emirates—but that revelation proved no great boon to the victim, Ahmed Mansoor. In the aftermath of the report, Mansoor lost his job, his passport, his car, his savings, and his freedom to the UAE security forces. He was beaten by unknown assailants twice in a single week. While Claudio, Donncha, Sandrine, and I sat in a comfortable flat in Berlin matching my contacts to numbers on the list, Mansoor was serving a ten-year prison term for threatening the “unity” of the state and damaging “the status and prestige of the UAE and its symbols.” He was reportedly being kept in solitary confinement and sporadically subjected to torture. “Mansoor’s wife, Nadia,” Reuters had reported in early 2019, “lived in

social isolation in Abu Dhabi. Neighbors are avoiding her out of fear security forces are watching."

The evidence already out there made things clear: Pegasus and other cybersurveillance systems had become favorite toys of some of the most vicious leaders in the world, men who would not hesitate to destroy the lives of anybody who crossed them. We were contemplating crossing them in a very big way.

When Claudio's automated matching program finished its work on my files, we went through the same exercise with Sandrine's. She had spent much of her early career in journalism covering politics, so her contact list was different from mine, which turned out to be helpful that day. A few French political figures in her contacts were also on the list of potential Pegasus targets. Then came the match that really jolted us: among several Mexican journalists in the data was Jorge Carrasco, the crucial lead partner in our current project.

Jorge's phone had likely been targeted by somebody in Mexican law enforcement or the Mexican military. But Pegasus was like loose nukes, gettable for the right amount of money, so it was also possible he was being watched by one or more of the corrupt and dangerous Mexican officials we were secretly investigating. Whoever had done the targeting might also be able to track us, and our team, and all the other collaborators on the Cartel Project, through Jorge.

We asked Claudio if Jorge should switch out his phone, and he said that was probably a good idea, but unlikely to solve the problem. NSO's customers could infect a new iPhone just as easily.

Sandrine contacted a colleague of Jorge's in Mexico right away and asked him to get a message to him: Jorge needed to replace his phone, and he needed to get off and stay off the Cartel Project Signal loop—immediately. We could not tell Jorge exactly why this was necessary, but he had to trust us. We would be in touch as soon as we had a new and secure way to communicate.

When Sandrine and I parted from Claudio and Donncha and started preparing for the long trip back home, we were left with two big questions:

How in the world could we do this story? And how could we not?