
RAUSCHER.XYZ
SEPTEMBER 22, 2026
AI GENERATED

RAUSCHER.XYZ

GOVERNMENT SPYWARE: SHOULD I WORRY?

A break-in that costs a fortune, aimed at almost nobody

In April 2018, Hanan Elatr was detained at Dubai International Airport, and her phone was taken from her. The next day, while the device sat in strangers' hands, someone typed a link into it. It took two typos and 72 seconds to enter that single line, a short string of characters that, if everything went right, would turn the phone into a listening post that traveled everywhere its owner went. The phone was an Android. Elatr would marry the Saudi journalist Jamal Khashoggi that June. That October he walked into his country's consulate in Istanbul and was killed inside it.

Investigators could reconstruct the attempt, but not its outcome. Whether the code ever took hold on Elatr's phone could not be established, in part because Android tends to leave an examiner fewer of the traces a later analysis leans on, and nobody at that keyboard is on record trying a second time. By contrast, Khashoggi's fiancée Hatice Cengiz was confirmed to have been infected after his murder. Either way, the effort circled the people closest to a marked man, and that detail has stayed with me longer than any exploit ever has.

I think about those 72 seconds every few weeks, since that is roughly how often someone asks me the question you probably came here with. Am I being watched by my own government? They have read a headline about Pegasus, about phones turned into microphones, and now a dropped call or a warm battery makes them suspect surveillance. They want me to sweep the phone, or at least to tell them how. I have spent many years pulling data off devices for courts, reading what others were sure they had erased, reconstructing a day from the traces a phone cannot help leaving behind. So they assume I will confirm the fear.

Usually I cannot, and I say so gently. The fear itself is not imaginary, even when the threat is. You are almost certainly not Hanan Elatr. The machine aimed at her phone costs a fortune to acquire and to keep running, and its value can fall sharply once the underlying flaw is found and patched, so its owners spend it with great care. There is real danger in this story. It simply does not live where the frightened person expects to find it, and telling the two apart is much of what I do for a living.

Later in this article, I discuss a piece of advice nearly everyone gives that sounds sensible but does the opposite of what people hope. Following it could hurt someone.

THE PRICE OF A KEY THAT FITS YOUR PHONE

If you want into a current iPhone without the owner touching a thing, you do not write that break-in over a weekend. You buy it, and the market rate is a matter of public record. In April 2024 the exploit broker Crowdfense posted a rate card, the sums it was willing to pay for working break-ins: between $5 and $7 million for a zero-click chain against an iPhone, and $3 to $5 million for one that gets in through a messaging app like WhatsApp or iMessage. Five years earlier the top of that market was $3 million. A Russian broker, Operation Zero, has publicly offered up to $20 million for tools that crack phones. These are advertised acquisition prices, what it costs to obtain the capability, not the cost of any single operation,

and that distinction matters. The figures show how highly brokers value a working exploit. They do not tell us what any government pays to acquire or to use one.

Set it against what a government pays to run the finished product. When the New York Times obtained NSO Group's price sheet in 2016, the figures read as quaint today: a flat $500,000 setup fee, then $650,000 to target 10 phones. Phones grew harder to open over the years, so the keys got more expensive, and the trade folded into the hands of the few firms that could still afford to forge them. A decade ago a single gifted researcher could sometimes assemble an iPhone chain alone. Today it takes a team, and teams cost money, which is much of why the price of a finished key keeps climbing instead of falling the way technology usually does.

The reassuring part follows from the same math. A key that costs millions to acquire and maintain does not get spent finding out whether you are lying about your diet. The numbers argue against it. These capabilities are costly to acquire and dangerous to expose, so those who hold them choose their targets with great care. For nearly everyone reading this there is no good reason to think we are on that list, and that, more than any setting on the device, protects us. None of that is flattering; it is an economic calculation, and for people like us it provides the most dependable protection we will ever have.

WHY THESE KEYS EXPIRE

The second reason the state handles these tools so carefully is the strangest thing in this grim trade. These keys have a shelf life, and it is shorter than the price tag suggests.

The zero-click chains I have been describing usually ride on a flaw the manufacturer does not yet know about, a hole nobody has patched, what the trade calls a zero-day. Once such a flaw is identified and a fix ships, the exploit loses reach with every phone that installs the update. The Paragon case shows the pattern from the defender's side. Apple says the flaw behind that spyware, cataloged as CVE-2025-43200, was closed in iOS 18.3.1 in February 2025, before Citizen Lab even published its findings that June. A capability that cost a fortune to build can be undercut by a security update its owners rarely think about. This is no clean one-way street. Attackers keep finding fresh flaws and other routes in, and unpatched phones can stay exposed for a long time, which is its own argument for keeping yours current. But an exploit that has been found and fixed is a wasting asset, and everyone in this trade knows it.

Their owners understand this, and it shapes how they behave. Fire one at the wrong target, at someone who happens to know a researcher, or who hands the phone to a lab on nothing but a bad feeling, and you may have set fire to your own investment. An examined phone can expose an exploit, and that risk may influence whom operators choose, but it has clearly not stopped them from going after journalists, activists, and senior officials. It does mean the capability is rationed, and the person most certain the government lives in his phone is rarely the one I end up worrying about. The ones who get hit tend to be quieter than that, and the few who catch it in time were already careful to begin with.

ONE MAN REFUSED TO TAP THE LINK

In August 2016 a human rights defender in the United Arab Emirates named Ahmed Mansoor received a text. It promised him secrets about torture inside his country's prisons, bait built for a man in his position. He had been burned before. Instead of tapping, he paused over the odd feeling for a moment, then forwarded the message to researchers at Citizen Lab and let someone else open it in a lab.

What waited behind that link was a chain of three separate iPhone zero-days, later cataloged as CVE-2016-4655, CVE-2016-4656, and CVE-2016-4657, wired together so that a single tap would have silently jailbroken his phone and turned it into an informant in his own pocket. Apple sealed all three in iOS 9.3.5 within days of being told. Citizen Lab's report gave Mansoor the phrase that stuck to the era afterward: the million dollar dissident. The name fit him all too well. He had been hunted with expensive tools before, first one commercial package, then another, then this one, three separate vendors' worth of spyware aimed at a single stubborn man who kept declining to disappear. His decision to forward the message instead of opening it let researchers identify three zero-days and led to a patch that protected a great many strangers who will never learn his name.

Sometimes the target sits at the very top. Spain's own government confirmed in 2022 that the phone of Prime Minister Pedro Sánchez had been infected with Pegasus in May of the previous year, and that more than 2.5 gigabytes of data had been drained from it. The defense minister's phone went the same way a month later, and the country's intelligence chief lost her post over the affair. Separately, Citizen Lab's CatalanGate investigation documented dozens of Catalan politicians, lawyers, and activists targeted with the same class of tools. When the same weapon can be aimed at the man who runs the country and at his political opponents, "the target is always someone else" starts to sound thin.

Sometimes it is simply a reporter who would not stop. In El Salvador, the journalist Carlos Martínez wrote that his phone had carried Pegasus for a total of 269 days across 2020 and 2021. Even spread across two years, it describes a phone that was, again and again, an open window onto a reporter's sources and a reporter's life. In Poland, two separate labs confirmed that the phone of an opposition campaign chief, Krzysztof Brejza, was broken into 33 times across the summer and autumn of a national election, and material taken from it was later used against him in public. This was never surveillance for anyone's safety. It was surveillance turned into a campaign tactic.

A COMPUTER HIDDEN INSIDE A FILE

You might picture a zero-click attack as brute force, a battering ram against a locked door. In practice it works like a locksmith operating blind, and the clearest example ever made public is the one Google's Project Zero took apart at the end of 2021, an exploit called FORCEDENTRY.

Stripped of jargon, the attachment arrived wearing the extension of a harmless animated image. It was really a PDF, and while the phone processed it, the file reached an ancient decompression format called JBIG2, invented decades ago to shrink scanned black-and-white documents down to a size a fax machine could stomach. JBIG2 cannot run a program. It cannot add two numbers together. It is a way to squeeze grainy pictures, an old tool for a dull job, and nothing more. And yet the attackers, using nothing but the small logical operations JBIG2 uses to compare one speck of a picture against another, built a working computer inside the file. Project Zero found a full processor, emulated out of more than 70,000 of these image-squeezing commands, running inside the step that was only ever meant to unpack a picture. The phone believed it was decoding an image. It was in fact executing a program its owner never saw, delivered inside a message he never opened.

The attackers built a computer using image-processing operations and ran it before anything appeared on the screen.

There is a companion case that is, if anything, colder. In 2023 the security firm Kaspersky discovered that its own employees' iPhones had been opened through a chain of four zero-days, and one of them relied on hardware registers that Kaspersky found were undocumented in the public material it examined, a feature of Apple's own silicon not written down anywhere an outside engineer could read it. Someone had found and used a door in the hardware that appeared on no public map. To this day no one has proven in public who that someone was, and I will not guess.

ADVICE THAT POINTS YOU THE WRONG WAY

Nearly everyone who worries about this assumes the danger is the exotic machinery, the zero-click, the secret register in the chip. So they reach for the obvious defense. Stop using the encrypted apps. Just make ordinary phone calls. Keep it plain and old-fashioned, and surely the spies lose interest.

That instinct has it backward, and the history shows why. End-to-end encryption is a large part of why authorities now reach for the device itself. For decades, police and intelligence agencies that wanted to hear you have been able to intercept an ordinary call at the carrier when a court authorized it. In the United States, CALEA requires the carriers to make that kind of lawfully authorized interception technically possible. In Germany, the same carrier interception is lawful, and the federal police describe it as requiring a judge's order. Then came WhatsApp and Signal and iMessage, where the message is scrambled on your phone and unscrambled only on your friend's, and the tap on the wire caught nothing but static. So the interest moved to the endpoint, to the phone in the hand. There a message can be read before it is locked or after it is opened, which is the one place the encrypted wire cannot hide it.

The advice to "just make ordinary calls" steers you back toward the one channel that authorities have long known how to intercept at the carrier, under whatever legal order their

country requires, without spending a cent on an exploit. The encrypted messenger you were about to abandon provided protection against that interception; ordinary calls never did. Whether that ordinary interception is easy or lawful in your case depends entirely on where you are and who is asking, and I am not going to pretend those rules are the same everywhere. Put narrowly, if a conversation has to stay private, end-to-end encryption is the thing protecting it, and walking away from it walks you toward the older, cheaper method instead.

A caution, because paranoia counsels worse than complacency does. Hardly anyone reading this will ever be intercepted by either method, for the cost reasons already covered. But if you sit in the small group that might be, at least face the right direction. The exotic attack is rare and ruinously expensive. The ordinary one is older, cheaper, and fenced in by rules that shift from country to country.

THE CUSTOMER LIST NOBODY WANTS TO READ

It is tempting to imagine one shadowy super-agency behind all of this. The truth is messier, and worse. This is an industry, with vendors and customers and invoices, and the customer list reaches into rooms you would not expect.

In the United States, where many of the readers of this blog live, the FBI bought Pegasus in 2018, tested it for roughly two years at a facility in New Jersey, and paid NSO Group about $5 million, and NSO built the Bureau a version, called Phantom, tuned to target American numbers. The Bureau says it decided against operational use in 2021. The DEA had earlier run an Italian tool, Hacking Team's Remote Control System, a fact that spilled into daylight when that company was itself hacked and 400 gigabytes of its secrets, client list attached, landed on the open internet in 2015. That same leak named the FBI and the United States Army as buyers.

In Germany, where I work, the Federal Criminal Police Office, the BKA, secretly bought Pegasus in 2019, took delivery in 2020, and began using it in 2021, and the government acknowledged the purchase only behind the closed doors of a parliamentary committee. The BKA's purchase is confirmed. I have seen claims that the domestic or foreign intelligence service uses the same tool, but I cannot verify them to the standard I would defend in court and will not present them as fact. What is not in dispute is that German law already contains the framework for this kind of on-device surveillance, split into a narrower source interception and a broader online search, each bound to a judicial order.

The rest of the map is uglier and well documented. Spain's intelligence service, whose director admitted spying on 18 Catalan independence figures. Poland's anti-corruption bureau, which bought Pegasus with money routed through a justice fund and turned it on the opposition. Greece, where the Predator scandal reached the national intelligence service, and where, in the associated criminal case, four people including the founder of the spyware maker Intellexa were convicted in 2026. Italy, where the domestic intelligence service used

Graphite against two migrant-rescue activists. Even Israel, home to more of these vendors than anywhere on earth, turned a tool inward: an official inquiry confirmed that its police used a version of Pegasus called Saifan under judicial warrants, and found instances in which the use went beyond what those warrants allowed. Mexico, NSO's first client, whose army ran a secret unit that spied on journalists and a human rights defender. Stack up the independent research and the footprint is sobering: Citizen Lab found indications of Pegasus operations in some 45 countries, products linked to the Intellexa alliance turned up in at least 25, and the older FinFisher tool in 32. The numbers describe a market whose customers are mostly governments in good standing.

WHAT I SEE WHEN I OPEN A PHONE

In my casework, the Android devices were usually the easier ones to get into once they were in my hands. Fragmented, patched late if at all, stranded on old versions of the operating system, carrying the compromises that pile up when a dozen manufacturers each cut their own corners. A current iPhone, on current iOS, powered off, has been a different matter entirely. Switched off, it has often left me with no realistic way in. I say it from the chair where I sat and failed: if privacy matters to you and you are choosing a phone, a current iPhone kept up to date is the stronger starting point, and if your worry is someone getting their hands on the physical device, powering it off is the single most effective thing you can do.

That last instruction sounds too simple to be true, but the mechanism behind it is easy to follow. The most important fact in phone forensics is the gap between a phone that has been unlocked at least once since it was switched on and one that has not. Before the first unlock after a restart, important classes of protected data are much harder to reach. The first unlock makes some additional data accessible, and some of that access persists after the phone is locked again, depending on the data's protection class. Extraction tools rely on that lingering access. This is not a quirk of one model or one season, and it is why the state of the phone, freshly booted or already unlocked once, matters more than anything else about it. Apple even slipped a small feature into iOS 18.1 that restarts a phone after it has stayed locked for a prolonged period, returning it to that harder state, a change the world noticed only when police evidence rooms full of seized iPhones began rebooting on their own. With the iPhone 17 in 2025 Apple went further, building memory defenses aimed at the chains we have been dissecting. None of this is a final victory. Nothing in this field ever is. It is an endless back and forth, and the other side is very well funded. But a restart does return the phone to its more protected before-first-unlock state, and it holds there until the next time its owner unlocks it, which is worth knowing on the day it matters. So that no one draws the wrong lesson: everything in this section is about physical extraction, about someone holding your phone in their hand. It is not a shield against a remote zero-click that arrives in a message while the phone is in your pocket. That is a different threat, and its defenses are the updates and Lockdown Mode, not the power button.

You do not need antivirus on your iPhone, and in the ordinary sense you cannot really have it, because Apple walls every app off from every other, so a consumer security app cannot rummage through other apps the way a desktop scanner does. Those iPhone security apps offer a VPN, a phishing filter, a breach alert, all useful, none of it the app-scanning antivirus you might picture, and none of it a reliable check for something like Pegasus. On Android the logic differs. The system is more open, and Google's Play Protect really does inspect apps across the device at a very large scale. Basic protection earns its place on Android. On iOS it does not. As for the serious corporate tool people sometimes bring up with me, CrowdStrike's Falcon for Mobile runs on both, but it is an enterprise product tied into an organization that manages the phone, reading device and risk signals instead of standing in for a personal malware scan, and it is not something a private person installs to guard a personal handset.

A SUSPECTED CASE ON MY DESK

The fear is almost always misplaced, and the word almost is carrying its full weight in that sentence. One case stays with me: I could not give the client a defensible yes or no, and it taught me a rule I still pass on.

It was an older iPhone, brought to me by someone convinced the state was inside it. I will not say who, because protecting the person is the point. Nor will I pretend it was a clean case, because it was not one. Early in the consultation I explained the uncomfortable truth, which is not what a client expects to hear from a forensic expert. A thorough examination could take considerable time and still leave us without a definitive answer. Proving that a sophisticated implant either was or was not present, to the standard I would defend in court, is hard on an aging device. After talking through those limits and what the client needed, I recommended the sensible course: set the phone aside, move to a clean device, configure it from nothing, and then learn from me how to talk to people from there on. The hardware was always replaceable. Helping the client develop safer habits was the more important work.

The device is the cheap part, and discipline does the protecting. For the small number of people truly in someone's sights, the discipline is specific and knowable. Run the latest operating system. Switch on Lockdown Mode, the feature Apple built for this threat. If physical seizure is a concern, power the phone off before it leaves your hands, so it returns to its most protected state. Keep it to as few apps as you can bear. And if a manufacturer ever sends you a credible threat notification, do not wipe the phone in a panic. It has just become evidence, and a lab can still read it. Apple and a handful of other companies do send these warnings, sparingly, and only to people they have reason to believe were singled out, so one is worth taking seriously rather than erasing on impulse.

THE FEAR AND THE PERSON CARRYING IT

A word about the emotion under all of this. I meet it constantly, and it deserves more than a joke at its expense.

Nearly everyone who comes to me about Pegasus shows no sign at all of being a target. They have an anxiety and a headline, and the two have found each other. So I start where the evidence usually leads, with the ordinary explanations, a failing battery, a buggy update, an account someone guessed from a password reused for years, and with the basic security of the device in front of me. In case after case, the trouble is somewhere in there, human and mundane and fixable, and the relief on a person's face when the cause turns out to be an ordinary settings problem is a good part of why I still do this.

In my cases, the people most certain they are being watched are rarely those at greatest risk. The person most sure he is under surveillance is usually the one for whom I can find the least sign of it. I do not say that to belittle the worry. The worry reflects a real danger in the world we live in, but misidentifies the threat to the person concerned. Part of my job is to explain that distinction gently, so the person can focus on updates and passwords instead of dread.

THE LOCK EVERYONE SHARES

Picture where the world is drifting. Everyone carries the same short list of devices. The same phone, or the same flavor of the other one. A single monoculture stretched across the planet. And a monoculture is a gift to any state with a budget: it means there is close to one lock in the world to pick, and the value of the master key grows with every person who standardizes onto the same lock as everyone else. That danger sits under all the individual horror stories. Not that your phone can be opened, but that everyone's phone is nearly the same phone.

Hardly anyone considers the way out, and it is why I do not despair. The mass market is a monoculture. You are not obliged to live entirely inside it. For an organization with the resources to maintain it, carefully vetted encrypted communications running on less common hardware, not the mass-market phone everyone else carries, may offer another path. A less common platform may make some widely reused exploit chains less useful to an attacker, which is an advantage, if a limited one. Whatever you build in place of the crowd still lives or dies by its design, its upkeep, and the hands that use it daily, and a seller promising 100 percent is selling you a feeling. But it does step you out of the single global lock, and for the handful who truly need that, the step is worth taking.

These tools are built by highly skilled people who can assemble a computer out of a fax format and exploit undocumented hardware features inside a chip. You will not outmuscle them, and you should not try. A more realistic aim is to understand the threat well enough to focus your attention where it is useful.

A warm battery is not evidence of spyware, and a dropped call is not a wiretap. Keep the phone updated, use a strong passcode for the phone and unique passwords for your accounts, and if you ever receive a credible warning, or have a real reason to believe you are a target, take it seriously and find someone who examines devices for a living. Short of that, the most rational thing to do with the fear is to turn it into updates and stronger passwords, and then let it rest.

DISCLAIMER

This article is for general information. The public cases discussed are based on the sources cited below. The account of my own work reflects my experience; identifying or ruling out a particular spyware infection requires an examination of the device and the circumstances. If you receive a credible threat notification or have specific evidence of targeting, seek qualified help before resetting or replacing the device. To the extent permitted by law, I accept no liability for any decision a reader makes based on this article.

REFERENCES

Al Jazeera. (2022, January 7). Polish leader admits country bought powerful Israeli spyware. https://www.aljazeera.com/news/2022/1/7/polish-leader-admits-country-bought-powerful-israeli-spyware

Al Jazeera. (2026, February 26). Greek court finds 4 guilty in major 2022 spyware scandal. https://www.aljazeera.com/news/2026/2/26/greek-court-finds-4-guilty-in-major-2022-spyware-scandal

Amnesty International. (2021, July). Forensic methodology report: How to catch NSO Group's Pegasus. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Amnesty International. (2023, October). The Predator Files: Caught in the net. https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-investigation-reveals-catastrophic-failure-to-regulate-surveillance-trade/

Business & Human Rights Resource Centre. (2021, September). Germany: Police reportedly bought NSO Group's Pegasus spyware in secret. https://www.business-humanrights.org/en/latest-news/germany-police-reportedly-bought-nso-groups-pegasus-spyware-in-secret/

Citizen Lab. (2015). Pay no attention to the server behind the proxy: Mapping FinFisher's continuing proliferation. https://citizenlab.ca/research/mapping-finfishers-continuing-proliferation/

Citizen Lab. (2016, August). The million dollar dissident: NSO Group's iPhone zero-days used against a UAE human rights defender. https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Citizen Lab. (2018). Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Citizen Lab. (2022, January). Project Torogoz: Extensive hacking of media and civil society in El Salvador with Pegasus spyware. https://citizenlab.ca/research/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

Citizen Lab. (2022, April). CatalanGate: Extensive mercenary spyware operation against Catalans using Pegasus and Candiru. https://citizenlab.ca/research/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

Citizen Lab. (2025, June 12). Graphite caught: First forensic confirmation of Paragon's iOS mercenary spyware. https://citizenlab.ca/research/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

Forbes. (2024, November 12). iOS 18.1: Apple secretly added a new iPhone security feature. https://www.forbes.com/sites/kateoflahertyuk/2024/11/12/ios-181-apple-secretly-added-a-cool-new-iphone-security-feature/

Globes. (2016, September). NSO Group charges $650,000 to hack ten iPhones, report says (reporting the New York Times price list). https://en.globes.co.il/en/article-nso-group-charges-650000-to-hack-ten-iphones-report-1001149988

Kaspersky. (2023, December 27). Operation Triangulation: The last (hardware) mystery. https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/

Lawfare. (2022). The Merari report on the Israeli police's Pegasus scandal. https://www.lawfaremedia.org/article/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal

Project Zero. (2021, December). A deep dive into an NSO zero-click iMessage exploit: Remote code execution. https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

R3D and Citizen Lab. (2023). Ejército Espía: Pegasus surveillance of journalists and human rights defenders in Mexico. https://r3d.mx/2023/03/07/estructura-secreta-del-ejercito-espio-con-pegasus-a-raymundo-ramos-con-pleno-conocimiento-del-secretario-de-la-defensa/

TechCrunch. (2024, April 6). Price of zero-day exploits rises as companies harden products against hackers. https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/

TechCrunch. (2025, June 12). Researchers confirm two journalists were hacked with Paragon spyware. https://techcrunch.com/2025/06/12/researchers-confirm-two-journalists-were-hacked-with-paragon-spyware/

The Intercept. (2015, July 6). Documents show FBI, DEA, and U.S. Army buying Hacking Team spyware. https://theintercept.com/2015/07/06/hacking-team-spyware-fbi/

The New York Times. (2022, November 15). Internal documents show how close the F.B.I. came to deploying spyware. https://www.seattletimes.com/nation-world/nation-politics/internal-documents-show-how-close-the-fbi-came-to-deploying-spyware/

The Washington Post. (2021, December 21). UAE agency put Pegasus spyware on the phone of Hanan Elatr, Jamal Khashoggi's wife. https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/

The Washington Post. (2021, July 18). Jamal Khashoggi's wife targeted with spyware before his death. https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/

KEYWORDS: state trojan, Pegasus, zero-click exploit, mercenary spyware, mobile forensics, encrypted communication, surveillance, iPhone security

IMPRINT

intelligent piXel GmbH
International Institute of Forensic Expertise (IIFE)
Enzianstraße 4a
82319 Starnberg, Germany

CONTACT

george@rauscher.xyz · Telegram @intelligentpixel

MANAGING DIRECTOR / AUTHORIZED SIGNATORY

Managing Director: George A. Rauscher
Authorized Signatory: Dr. Louise Morgott

RESPONSIBLE FOR JOURNALISTIC AND EDITORIAL CONTENT

Responsible for journalistic and editorial content pursuant to Section 18(2) of the German Interstate Media Treaty:
George A. Rauscher, c/o intelligent piXel GmbH, Enzianstraße 4a, 82319 Starnberg

VAT ID NO. / COMMERCIAL REGISTER

VAT ID No.: DE291416044
Commercial Register: HRB 207 679, Munich District Court

© 2026 GEORGE A. RAUSCHER · IIFE