

The Surveillance Empire That Tracks World Leaders, a Vatican Enemy, and You

Inside the hidden world of untraceable tech has targeted politicians, journalists, celebrities, and activists around the globe.

GABRIEL GEIGER, CROFTON BLACK, EMMANUEL FREUDENTHAL, AND RICCARDO COLUCCINI

“The problem is the export license, huh? For this we can find a...a way.”

It was early June and Guenther Rudolph was in an expansive mood. Sharp-suited, relaxed, and charming, he was standing in a booth in Prague’s Clarion Congress Hotel. Every year the Clarion hosts an exclusive gathering: the premier get-together of the surveillance industry, called ISS World Training, where law enforcement and intelligence officials from across the globe mingle with representatives of leading spy companies. People outside the business—including journalists—are barred from entry.

On the hotel’s first floor, vendors lined up to sell their wares, and digital displays pulsed with inspiring slogans: “eliminate the unknown,” “saving lives.” Products ranged from hidden cameras to drones to “open source intelligence” and “AI-powered analytics.” But the largest, glitziest, and busiest booths advertised access to people’s phones.

Some of the companies that have promoted their products at this event are now infamous, such as NSO Group, which makes the blacklisted Pegasus spyware that news reports and multiple lawsuits implicated in Jamal Khashoggi’s murder, or Intellexa, which triggered a hacking scandal in Greece. In recent years, surveillance companies have been linked to assassination plots. They have been exposed for targeting politicians, including members of Congress; political dissidents and human rights advocates; and journalists. Their spy ops have led to lawsuits, parliamentary inquiries, financial penalties, and, in the case of both NSO Group and Intellexa, US government sanctions. But, through these controversies, one company has remained in the shadows.

Rudolph is its sales director, and in Prague he was considering a proposition from Albert, the South Africa-based owner of a “boutique research consultancy,” with an address in the popular tax haven of the British Virgin Islands. Albert was accompanied by his top client, a well-heeled Nigerien mover-and-shaker named Abdou.

Over the course of the three-day conference, the three men met several times and spoke for hours about what Rudolph’s company could do for Albert and Abdou’s customers. Could his company help them identify, profile, and track environmental activists protesting a mining concession, they asked in one conversation? It could. Could it help a West African government monitor citizens traveling abroad? Indeed. Could it access encrypted WhatsApp chats? “Easily,” said Rudolph.

But, Rudolph pointed out, there was a potential snag. In addition to export laws that restrict the sale of surveillance tech in certain countries, some of their customers may be under sanctions imposed by Western governments. “If you are holding an Austrian passport, like me, I am not even allowed to know about the project. Because otherwise I can go to prison.”

Rudolph had a solution.

“So that’s why such a deal, for example, we make it through Jakarta, with the signature coming from our Indian general manager.” His hands acted out putting the deal somewhere else, off to one side, out of sight. “We will never know about this project,” he concluded, with a hint of a smile.

Rudolph was unaware that he was talking to two undercover reporters. What brought them to his sales booth at a hotel in Prague is a story that starts more than 20 years ago, when the company where he works, First Wap, was set up in Indonesia. Ever since then, First Wap has operated entirely under the radar—avoiding the fate of competitors in the industry.

“They are all so public, you can read about them in the newspaper, you know,” Rudolph cautioned. “This is not good.”



Scenes from the ISS conference in June.

Clockwise from top left: Lighthouse reporter Emmanuel Freudenthal (“Albert”) prepares to go undercover; Guenther Rudolph, First Wap’s sales director; First Wap execs provide a demonstration of Altamides; Evgeni Karakanovsky, general manager of First Wap.

Operating from their base in Jakarta, where permissive export laws have allowed their surveillance business to flourish, First Wap’s European founders and executives have quietly built a phone-tracking empire, with a footprint extending from the Vatican to the Middle East to Silicon Valley.

It calls its proprietary system Altamides, which it describes in promotional materials as “a unified platform to covertly locate the whereabouts of single or multiple suspects in real-time, to detect movement patterns, and to detect whether suspects are in close vicinity with each other.”

Altamides leaves no trace on the phones it targets, unlike spyware such as Pegasus. Nor does it require a target to click on a malicious link or show any of the telltale signs (such as overheating or a short battery life) of remote monitoring.

Its secret is shrewd use of the antiquated telecom language Signaling System No. 7, known as SS7, that phone carriers use to route calls and text messages. Any entity with SS7 access can send queries requesting information about which cell tower a phone subscriber is nearest to, an essential first step to sending a text message or making a call to that subscriber. But First Wap's technology uses SS7 to zero in on phone numbers and trace the location of their users.

First Wap emphasizes that its technology is used by law enforcement to “fight against organized crime, terrorism and corruption.” It sells Altamides directly, as well as through third-party resellers. The company said in a statement that it does not provide “any tracking services to government entities or similar”—that is, it does not perform any tracking itself—and that “after installation” it has no further involvement in or knowledge of how its product is used. It said it sells solely to “government entities, which have a clear and verified legal mandate to obtain and operate such products” and it “vets and verifies” users “for sanctions compliance.” The company's contracts state that customers must comply with anti-corruption laws and “there must not be any business transaction with a sanctioned entity,” and First Wap said it adheres to these rules “no matter what any sales personnel may state verbally.” Of the company's interactions with undercover reporters at the Prague conference, it said that “misunderstandings evidently arose” and that the statements by its executives referred merely to “technical feasibility.”

Last year the investigative newsroom **Lighthouse Reports** obtained a secret archive, containing more than a million instances where Altamides was used to trace cell phones all over the world. This data trove, the majority of which spans 2007 to 2014, is one of the largest disclosures to date of the inner workings of the vast surveillance industry. It does not just list the phone numbers of people who were monitored; it offers, in many cases, precise maps of their movements, showing where they went and when. Over months of research, Lighthouse, Germany's **Paper Trail Media**, *Mother Jones*, *Reveal*, and an international consortium of partners dug into these logs to understand who was being spied on and why. We identified surveillance targets in 100 countries and spoke to dozens of them. We obtained confidential documents and communications outlining how Altamides—an acronym for “Advanced Location Tracking and Mobile Information and Deception System”—was marketed and deployed. We also interviewed industry insiders and former employees of the company about its operations and clientele.

What we found changes what we know about the history of surveillance technology, demonstrating the proliferation of dangerous tools well before Edward Snowden brought the issue to global attention. Despite its considerable size, the archive represents only a fraction of the surveillance activities carried out with Altamides. But it nevertheless shows how it was used, and abused, across the world.

The First Wap archive reveals extensive cell phone tracking in the US, which usually is considered out of bounds for spyware and surveillance vendors. Even the most notorious, like Israel's NSO Group, have made a point of avoiding it. Foreign companies that have surveilled people in the US have in multiple cases been sanctioned. Yet Altamides was deployed in thousands of tracking operations on US soil.

“What's happening here is a very specialized industry that's enabling some of the world's worst dictators and despots to undermine the foundational pillars of liberal democracy.”

The targets included Blackwater founder Erik Prince (who declined to comment), executives from military contracting company Raytheon, employees of telecom and cybersecurity firms, and a foreign defense attaché based in Washington, DC. Altamides pinpointed the location of Google engineers as they traveled across Northern California, and it tracked Anne Wojcicki, founder of DNA testing startup 23andMe who was then married to Google's Sergey Brin, more than 1,000 times as she moved across Silicon Valley and San Francisco. (Google declined to comment, while Wojcicki told us she had no knowledge of these efforts to track her.) Award-winning journalist and former CIA lawyer Adam Ciralsky's phone was targeted as he investigated the arms industry for *Vanity Fair*. A phone number that public records link to Hollywood star Jared Leto was targeted a month before he began filming *Dallas Buyers Club*.

Sen. Ron Wyden (D-Ore.), who has raised the alarm about the security of US telecom networks, said the findings of this investigation “underscore the glaring weaknesses in our phone system, which the government and phone companies have failed dismally to address,” and noted that the current and former administrations have “refused to release a damning report about telecom security vulnerabilities while foreign hackers spy on executives and government officials with impunity, making all Americans less safe.”

Elsewhere in the world, the First Wap archive shows how the company's technology was used by repressive regimes, as well as by corporate investigators. It has even been utilized for personally motivated invasions of privacy. The onetime prime minister of Qatar, the ousted first lady of Syria Asma Al-Assad, high-profile international lawyers, music stars, and executives all came into Altamides' crosshairs. But we also found hundreds of people with no public profile swept up in the dragnet: a softball coach in Hawaii, a restaurateur in Connecticut, an event planner based in Chicago.

“You have a company that has been able to operate in the shadows without any public accountability or transparency,” said Ron Deibert, director of the Citizen Lab at the University of Toronto, an organization that helped to expose the Pegasus spyware and in recent years has been at the forefront of researching surveillance technology and its impacts. “What's happening here is a very specialized industry that's enabling some of the world's worst dictators and despots to undermine the foundational pillars of liberal democracy.”

For many people, their cell phone is their most essential possession. It knows everything about them and follows them wherever they go. The security risks when this information gets into the wrong hands are therefore profound. Tracking, hacking, or snatching data from phones is a highly prized—and priced—capability.

The industry has argued long and loudly that these expensive and invasive tools are closely restricted to a tight circle of government users and uses. Our year-and-a-half-long investigation into First Wap dismantles that argument. What emerges is a very different picture of how such tools have proliferated without restraint.



In July, Gianluigi Nuzzi settled into an armchair at his exclusive members' club, Casa Cipriani in Milan, and peered at a map on a laptop. No stranger to intrigue as an investigative reporter, he suddenly realized the import of what he was seeing. "In Chinatown...move a little more, that's it. Wait, stop. Via Venafro, here."

We were showing Nuzzi a query that, in 2012, had come through to Nuzzi's mobile phone operator, San Marino Telecom, probing the Italian network to identify the antenna that Nuzzi's phone was nearest to. The network had responded with a string of digits, which in turn led to this point on the map. Looking at the location it identified took Nuzzi back more than a decade, to his old apartment, and to a time of fear and stress.

In May 2012, Nuzzi was launching his new book, *His Holiness: The Secret Papers of Benedict XVI*, a set of stunning revelations about corruption in the Vatican. For a year he had lived with the secret that he was carrying around a USB stick of Pope Benedict's personal documents. When the book finally appeared, he felt he could at last relax.

But his newfound sense of ease was premature. On the day of the book's publication, just after 10 a.m., the first attempt to locate his phone occurred. Over the coming days, more than 200 such attempts followed. It happened entirely without Nuzzi's knowledge.

"I just remember seeing it for the first time, I was stunned, I was absolutely stunned." Reconstructed years after the event, his travels are fastidiously mapped by First Wap's tech. We see him in Milan; on the motorway passing Piacenza; outside Bologna; in Rome, at the airport and in the historic city center near the Trevi Fountain. Sometimes his movements are charted in fine-grained detail, hour by hour or even minute by minute.

On May 23, 2012, a week after First Wap started tracking Nuzzi's movements, the Vatican police arrested Pope Benedict's butler, Paolo Gabriele, on a charge of stealing the pope's private papers and leaking them. The next day, the tracking stopped.

How did a European-led company in Indonesia become entwined with the work of an Italian journalist digging into the secrets of the pope? The answer takes us deep into the hidden world of First Wap.

READ MORE COVERAGE FROM OUR PARTNERS

- Surveillance Secrets —Lighthouse Reports
- First Wap, a discreet cyber-surveillance firm tracking journalists, public figures and corporate executives —Le Monde
- Die dubiosen Geschäfte einer Überwachungsfirma —Der Spiegel
- NRK avslører: Tidligere Telenor-topp blant tusenvis utsatt for sporing —
NRK

- First Wap, the pioneer of surveillance companies you've never heard of — [IрпиMedia](#)
- Big Brother from Austria: The company that monitored cell phones worldwide — [Der Standard](#)
- 300 Israelis under surveillance: Who spied on arms dealers, spy manufacturers and the prosecutor in the Netanyahu case — [Haaretz](#)
- Međunarodno istraživanje „Tajne nadzora”: špijunskim softverom „Altamides” praćeni srpski biznismeni — [KRIK](#)
- Überwachung: Massen-Missbrauch von Handyortung? — [ZDF](#)
- Zehntausende Handys wurden weltweit illegal überwacht – auch in der Schweiz — [Tages-Anzeiger](#)
- Investigasi: Jejak Pelacakan Nomor Telepon Aktivist dan Tokoh Publik — [Tempo](#)

In 2013, **Edward Snowden** unleashed a deluge of evidence about the National Security Agency's hacking tools. These highly classified techniques and exploits were, at least in theory, available to no one other than the US government and its “five eyes” partners, members of an exclusive anglophone geopolitical axis: the United Kingdom, Canada, Australia, and New Zealand.

But while Snowden's revelations ignited a firestorm over the legality and proportionality of government surveillance, especially in the US, they obscured a more fundamental truth. Over the previous years, a nascent private industry was already beginning to tap into the potential of a globalized market. Not all governments had the capacity to build their own surveillance infrastructure; some just wanted to buy it off the shelf. Quietly building a niche at the forefront of this industry was a man who until now has remained unknown even among surveillance experts. He was an Austrian who had immigrated in the 1990s to Indonesia and there set up two outfits: an NGO supporting disadvantaged children, and a mobile phone messaging service. His name was **Josef Fuchs**.

Fuchs, who died in 2024 at the age of 69, hailed from the Tyrolean Alps, on the border of Italy and Austria, and cut his teeth as an engineer for German industrial powerhouse Siemens. In 1995 he was in Jakarta, working for a local mobile phone operator. By 1999, he had founded First Wap. The “WAP” in the name stood for “wireless application protocol,” a once-cutting-edge mobile internet technology. WAP was soon obsolete, and while the company kept the name, its business swiftly pivoted to a different set of products and customers. According to First Wap, its transformation was spurred by an unspecified law enforcement agency that had asked the company whether it “could develop a product” to support its counterterrorism efforts. Within a few years, First Wap was no longer focused on sending

marketing messages. It had become a phone-tracking lab, one that boasted it could locate anyone anywhere on earth.

The world's police forces have long had legal access to records of communications within their own jurisdictions. In the mobile phone era, this includes location data, since every mobile phone interaction relies on a tower situated in the vicinity of the person communicating. But First Wap offered something different: instantaneous, global, and remarkable, even to industry insiders.

"I just remember seeing it for the first time, I was stunned, I was absolutely stunned," said one former sales executive, who gave demonstrations of First Wap's tools to potential clients around the world. Like other insiders we interviewed, he asked for anonymity, given his involvement in the secretive industry. "The thing about the First Wap system is that you could access it from anywhere in the world," he said. He also recalled a "scary" lack of control over who used it and for what purposes.

The company provided access to Altamides via an onsite hardware installation linked to a local telecom carrier to which the customer, presumably a government, had access. But it also had a web portal that it used to demonstrate its product. That portal relied on SS7 connectivity through an Indonesian telecom carrier and via Liechtenstein's national operator, with which it had a long-standing relationship dating back to its days in the SMS marketing business. The First Wap archive shows that Altamides routed hundreds of thousands of location-tracking queries—including those targeting Gianluigi Nuzzi—through Telecom Liechtenstein.

The phone carrier said it was unaware of any misuse of its network by First Wap. "Due to the serious allegations, Telecom Liechtenstein has immediately suspended its business relationship with First Wap," a company spokesperson said. "If the allegations are substantiated, the collaboration will be terminated without notice, and the company reserves the right to take legal action."

In the last decade, a number of companies have developed products exploiting the SS7 system for surveillance purposes. First Wap, industry insiders said, was the first.

"They were ahead of their time," said a former manager who worked at First Wap in the early 2000s.

WHO WAS TRACKED



Altamides targeted a phone linked to actor **Jared Leto** four times in 2012.



Five tracking attempts were made on a phone associated with **Asma al-Assad**, the ousted first lady of Syria, in 2013. Attempts were also made to track the phone of her sister-in-law.



In 2009, 23andMe founder **Anne Wojcicki** was tracked more than 1,000 times.



In 2013, 18 attempts were made to track a phone linked to **Hamad bin Jassim bin Jaber Al Thani**, the former prime minister of Qatar.

When we cold-called dozens of First Wap's targets, some thought it was a scam, and others wanted to know if they were still being tracked. Most people were baffled, shocked, or angry when they learned what had happened. But for some, the revelation that they or their close relatives had been surveilled through their mobile phones sparked no surprise at all. Such was the case for David Batenga, the nephew of Rwandan intelligence chief turned dissident Patrick Karegeya.

Batenga recalled pacing the lobby of the Michelangelo Towers hotel in Johannesburg on New Year's Day in 2014, waiting for word from his uncle. The hotel staff told him Karegeya was resting. A "do not disturb" sign hung on the door and his uncle's feet on the bed were visible to a staff member who peeked in. But he was not resting. He **had been strangled**.

A few years earlier, Karegeya had fallen out with Rwanda's president, Paul Kagame, and fled to South Africa. There, he had been working with other dissidents and former soldiers to build a new political opposition in exile. Batenga recalled the energy of that time: Karegeya and his allies were starting to build what they thought could become a real alternative to the Kagame regime, known for its repressive rule and the assassination campaign it has carried out against political opponents. "The momentum was growing stronger and stronger," he said.

"Locations are very important...All those phones are very essential for the eventual killing of someone, you know."

Karegeya was joined in South Africa by the former chief of the Rwandan army, General Faustin Kayumba Nyamwasa. A 2010 assassination attempt on General Kayumba linked to the Kagame regime almost succeeded. The same year, another former soldier, **Robert Higi**ro, received a phone call with an order from Rwanda's military intelligence chief. "Go to South Africa and eliminate Colonel Patrick and General Kayumba," Higiro remembers him saying. "Just like that on a direct line."

Higiro, who warned Karegeya and Kayumba, played along, taping conversations in which the murder plot was discussed. But as he kept the conspirators talking, other plans were afoot.

In January 2012, Altamides zeroed in on a phone belonging to Karegeya's driver and bodyguard, Emile Rutagengwa. Later that month, General Kayumba's wife, Rosette, was targeted multiple times by the location-tracking tool. In May, it was again Rutagengwa's turn. Someone was using Altamides to try to pinpoint the general and the former spy chief, by following the people closest to them.

The archive, large though it is, offers only an incomplete snapshot of Altamides' tracking efforts, and contains no further targeting of these people over the next year, so it's not clear what role if any Altamides may have played in Karegeya's assassination. A spokesperson for the government of Rwanda said that "Rwanda has never had nor sought to have such software, directly or indirectly." South African investigators linked Karegeya's murder to the Kagame regime, but the suspects of his killing remain at large.

“Locations are very important,” Higiuro told us. “You need to be tracking everyone that is close to them. If you know their bodyguards, if you know their spouses, if you know their kids. All those phones are very essential for the eventual killing of someone, you know.”

Fuchs’ company had no qualms about striking deals with repressive and autocratic regimes, former employees say. “We have to trust they would use it for ethical reasons,” said one, referring to how First Wap performed customer due diligence. Another confirmed: “There were no red lines as to which countries they sold Altamides to.” First Wap said in a statement that it “denies any illegal activity” or “human rights violations” and that “strict obligations of client confidentiality prevent us from addressing specific allegations.”

The company did not always sell to governments directly. It also tapped a network of resellers to market Altamides across the world. We obtained confidential documents showing how a British company, KCS Group, along with its subsidiaries and related companies, pitched First Wap’s system to numerous governments with poor human rights records.

KCS stands for Knightsbridge Company Services, named after the upmarket part of London synonymous with Harrods, Hyde Park, and Buckingham Palace. It was mainly known as an investigations outfit for companies and wealthy individuals. Its founder was Stuart Poole-Robb, described in his online CV as a former serviceman in the Royal Air Force, a karate instructor, and a provider of “specialised corporate and cyber intelligence.”

“This is essentially despotism as a service.”

Poole-Robb became aware of Altamides in 2010 and sought rights to sell it in certain markets, reaching out to people in high places to see if they could help drum up business. He surmised that he could charge more than \$3 million for it. It was, he emailed a colleague, “a high priced item with very significant margins.”

“Altamides will be used by governments which brings into question civil rights issues,” he added. “But then that is their problem not ours!”

In response to a detailed list of questions about the KCS Group’s involvement with First Wap and Altamides, Poole-Robb stated that the company “has not been involved in selling or using inappropriate surveillance materials” and is “committed to maintaining ethical standards in all our operations.” He added, “While I cannot disclose specific details concerning our clients due to confidentiality agreements, I assure you that the claims regarding our involvement are inaccurate.”

The initial “cooperation agreement” that KCS Information Services signed with First Wap in May 2011 gave Poole-Robb permission to market Altamides in Syria, where the revolution had just begun, and in Saudi Arabia. In a telephone call, Poole-Robb denied the existence of this agreement, a signed copy of which we obtained.

Poole-Robb said KCS Group “never marketed First Wap’s Altamides” and had never spoken to any governments in relation to it. Documents we obtained show how, as the Arab Spring roiled the Middle East and North Africa, the company began pitching Altamides heavily to Algeria and Morocco, as well as to the governments of Thailand (which had been taken over by a military dictatorship that brutally cracked down on the red-shirt protest movement), Sierra Leone, and Bangladesh.

In the aftermath of public unrest in Bahrain that led to the cancellation of the 2011 Formula One Grand Prix, Poole-Robb explored offering the tool to the Bahraini royal family to “help toward identifying ‘negative elements’” and “combat negative press and media.” KCS also considered a proposal—ultimately shelved—to offer the tool to a shipping protection company working in Gabon and Somalia. An email to Poole-Robb about this idea noted that staff needed to “put thinking caps on” about ways to give Altamides to a “third world country” with “a security company actually running the service,” adding that there were “all sorts of legal and funding issues.”

The numbers were tempting. Although KCS could offer a stripped down version of Altamides to Bangladesh’s intelligence agency for just over \$1 million, a full version of the system for the Algerian military intelligence department was priced at almost three times that.

KCS staffers were gung ho about sales. “I see an awesome lot of GBP and £ signs :)” wrote one. “Hope to see an awful lot of monies coming in soon :D”.

First Wap, too, supported KCS’s sales efforts, at one point offering Poole-Robb a discount “if it helps you to sign your first Altamides contract.” But the efforts kept getting bogged down.

“Altamides will be used by governments which brings into question civil rights issues. But then that is their problem not ours!”

Sales agents quibbled over margins. Customers demanded demonstrations and then went quiet for months or failed to fill in paperwork. Procurement budgets were delayed and technical hitches needed fixing. Shadowy middlemen demanded urgent conference calls that ultimately seemed to be fishing expeditions to get information about the product.

One reason it was tricky was that KCS was not the only reseller scrabbling to get an Altamides sale across the line. First Wap engaged numerous resellers to market its product.

The First Wap archive provides a detailed account of the movements of its resellers, since they often tested the system on themselves and their colleagues while giving demonstrations to potential clients. The data does not show which of these possible clients ended up making a purchase. But it offers a day-by-day map of the globetrotting itineraries of First Wap’s salespeople.

First Wap’s network of resellers included Germany’s **Elaman**, ThorpeGlen, headquartered in the UK, and **Gamma Group**, based in the UK and Germany. Executives and staff from these companies used Altamides to locate themselves or their colleagues in, among other places, Equatorial Guinea, Turkmenistan, Yemen, Oman, and Jordan. (ThorpeGlen and Gamma Group are now defunct. Elaman said in a statement it “never sold, offered, or implemented” Altamides.)

According to documents and interviews with former employees, Altamides customers included Belarus, Indonesia, Malaysia, Nigeria, Saudi Arabia, Singapore, the UAE, and Uzbekistan. “[T]his is an extraordinary tracking system that is proving itself very effective in over a dozen countries from Singapore to Nigeria,” Poole-Robb boasted in a 2013 email to a prospective client in Bangladesh. Representatives of these countries did not respond to requests for comment.

Citizen Lab’s Ron Deibert said this client list reads like “a rogue’s gallery of human rights abusing, authoritarian countries.”

He added, “This is essentially despotism as a service.”

First Wap said it had “not offered or sold” its products to “repressive” regimes. “Whether and to what extent the company’s late founder, Josef Fuchs, held discussions with potential interested parties or announced presentations in this regard is no longer verifiable,” the company said. “We have no knowledge of this.”

Autocratic regimes buying powerful surveillance tools barely raises eyebrows these days. But one nation’s interest in them still does.

The Vatican, or “Holy See,” is the world’s smallest state, both in area (smaller than the National Mall in Washington, DC) and population (about 1,000 people). But it was not too small to be a potential government client for Altamides.

Documents and tracking data we obtained show that in 2012 and 2013, KCS Group aggressively pursued a sale there. Referenced internally by different circumlocutions—“the V”, “pope city”—it was a continual topic of discussion within the company. Italian journalist Nuzzi, at this moment the Vatican’s public enemy number one, was a fulcrum of the sales pitch. In early May 2012, KCS’s pointman for Italy sent a message to Poole-Robb, the company’s CEO, confirming a meeting in Milan with “the ‘V’ people” for an Altamides presentation. He added: “I will ask them to provide us with the phone numbers to check asap.”

Poole-Robb said that his company “certainly didn’t” offer Altamides to the Vatican and that he was unaware of a meeting taking place between his firm and Vatican officials.

The day before the meeting, First Wap executive Jonny Goebel wrote to KCS saying that a First Wap employee “will set up a tracking” for two Italian phone numbers for KCS to showcase at the Milan presentation. The numbers belonged to Nuzzi. Their locations, mapping where Nuzzi went over a seven-day period, were part of the pitch for “the V people,” which was given just as the Vatican police were closing in on Nuzzi’s source. As he was on his way to the meeting, KCS’s Italian pointman was still requesting additional tracking assistance from First Wap. A few hours later, he wrote back to the Indonesian company with an update: “Client happy anyway...”

First Wap said that all its geolocations were done “in connection with presentations and with the consent of the persons involved. There was no misuse on our part.” Whether resellers had misused its product, the company added, was “beyond our knowledge.”

The correspondence between First Wap and KCS contains no record that anyone raised questions about whose numbers they were tracking for the Vatican, or why. The Vatican did not respond to a detailed request for comment or answer questions about who gave KCS Nuzzi’s phone numbers or how the tracking information derived from them was used.

“It’s disturbing,” Nuzzi said, seeing the evidence of how his movements were exposed. “We should track enemies, not journalists.”



In order to enable field personnel to have the same operational capabilities as ALTAMIR's users in the resolution center, the mobile

Global Operations

Altamir Global Operations

There was one line that the burgeoning private surveillance industry has generally refused to cross. Governments, however reckless or repressive, were seen as fair game. But private clients were off limits. Yet Altamides has made its way into private hands.

In 2013, KCS was preparing a “discreet due diligence” report on oil and gas executive Roberto Casula, who worked at the Italy-based energy multinational Eni. This report, which was sent to Eni’s security head Umberto Saccone, sought information to discredit Casula, including allegations of bribery and criminal association. It was the type of dossier often commissioned from a corporate intelligence firm. But the KCS report came with a twist: “Technical surveillance revealing recent movements.” KCS had used Altamides to track Casula in Italy and on a trip to Libya.

KCS’s Poole-Robb said he “100 percent” denied tracking Casula using Altamides and noted that his company “never used location tracking for anyone in relation to that type of work.” He added, “We tend to work where possible on the side of the angels.” Eni said in a statement that Casula and Saccone “have not worked at Eni for several years” and that it “is not aware of the specific matter and has no further comments on it.” Neither Casula nor Saccone responded to requests for comment.

KCS also deployed Altamides for private clients in other instances: to surveil Italian venture capitalist Alessandro Benedetti on behalf of Egyptian billionaire Naguib Sawiris during legal wrangling over a telecom deal, and to track Formula 1 journalist Joe Saward in order to learn if someone was paying him for his critical coverage of Team Lotus. Sawiris did not reply to multiple requests for comment. Dany Bahar, the Lotus executive the Saward report was presented to, said that he had “no knowledge about any surveillance tracking software and such practices nor would I approve such means.”

“I feel very vulnerable. Like there is no privacy, there is no private safe space where I can just be left alone.”

Cases like these show how easily, once access is given to a powerful location tracking system, its use expands beyond intelligence agencies and law enforcement. Sneaking into phone networks and using them to elicit intelligence about business competitors, litigation opponents, and others becomes another tool in the corporate arsenal.

But even more troublingly, the First Wap archive shows how Altamides was used for purely personal reasons.

Sophia (not her real name) was perplexed when we told her that her old phone number popped up in the logs of a military-grade location tracking system. She was followed for almost a year: at the office, at her home outside London, and even as she walked the beaches of Goa on a rare vacation.

At first she speculated the surveillance might relate to her job—business intelligence for a pharmaceutical multinational—or her background, a Russian immigrant who had been publicly critical of Vladimir Putin and his government. But as she pieced together the story, revisiting old Facebook contacts and assessing the data pattern we found, a disturbing truth emerged.

On arrival in the UK, she needed a new driver’s license. Her company contracted a driving instructor, who gave her lessons while regaling her with stories of his alleged time in the Pakistani military. At first she found him talkative, charming, helpful even. But over time, what had seemed like friendliness

began to feel like pursuit. Sophia rebuffed his advances and eventually cut ties with him. But, she said, he continued to call and text her.

Spurred by the recollection, Sophia took another look at her former driving instructor. And she uncovered a crucial detail, which she passed on to us. “A guy with the same name seems to represent a Pakistani surveillance and forensic technology company,” she wrote.

The company was a leading provider of security products to Pakistan’s armed forces. Her driving instructor was one of its sales managers. The First Wap archive shows that Sophia was targeted within minutes of several of his close professional and personal associates, indicating that he was testing the tool on all of them.

A year after she was tracked, Sophia moved from the UK, keeping her old phone number as she resettled. As she prepared to disconnect her number, she listened back to unopened voicemails. One of them was her driving instructor confessing that he had “done wrong things” and “crossed a line.”

More than a decade later, knowing that she was tracked, those comments took on newfound significance. “I feel very vulnerable,” she said. “Like there is no privacy, there is no private safe space where I can just be left alone.”

First Wap has continued to develop Altamides, adding new capabilities. Now it can not only track locations, it can intercept calls and messages and crack accounts that rely on passcodes sent via text messages—including the encrypted messaging service WhatsApp, as Guenther Rudolph told Albert and Abdou, the Lighthouse reporters posing as potential buyers, at the ISS conference in June. The company steers clear of the spyware, highly regarded in the industry, that provides access to everything on a target’s device. It continues to exploit phone networks, which offers more limited surveillance possibilities, but allows First Wap to operate more freely and flexibly than its competitors, Rudolph said.

Expensive hacking tools, he explained during one conversation with Albert, are too short-lived. “As soon as Apple get informed that there’s a vulnerability, they close it with the next patch. So whatever you buy now, in two months you can put your money in the garbage bin.”

Additionally, he said, the media attention that high-end hacking tools have attracted has meant that their vendors now have “ethical principles.”

“They don’t want to get into the newspaper or into the internet and be, okay, another president in Africa who is monitoring the free press or restricting human rights or whatever. So they don’t want this right? Bad marketing for them.”

Rudolph mentioned an Israeli hacking firm, sanctioned by the US on the basis that it had supplied spyware used to target journalists, businesspeople, and activists. Rudolph said he had introduced two new clients to the firm, only to have them rejected—representing a loss to the Israeli firm of tens of millions of dollars of potential business.

“I said, ‘Not bad!’ So they just dumped 100 million, huh? I also want to have this moralistic viewpoint.”

Across hours of discussion over multiple days at the Prague conference, one theme emerged repeatedly, echoing the findings from the First Wap archive: First Wap was prepared to do business with places—and people—that should have been off limits.

“We emphatically reject any allegations that we offer an illegal business model or promote, support, or enable unlawful operations,” First Wap said in a statement.

One scenario Albert and Abdou discussed with Rudolph in detail was that of a mining company facing problems from environmental activists looking to disrupt its business. How could First Wap help their West African client? Rudolph’s response was pragmatic. “He knows already who are the leaders, or he wants to find out?”

“They don’t want to get into the newspaper or into the internet and be, okay, another president in Africa who is monitoring the free press or restricting human rights or whatever.

So they don’t want this right? Bad marketing for them.”

The mining company would need to organize connectivity with a local phone operator, which typically means that someone in government has to sign off. But “if they could bring us the connectivity, then we can deliver,” Rudolph said.

Other companies would not do this, he added, because it would contravene laws around exports of surveillance technology that are in force in Europe, Israel, and America—but not in Indonesia.

“I think we’re the only one who can deliver,” he said.

The next day, Rudolph, along with Jonny Goebel, now First Wap’s owner, described how they could structure the delivery of a tracking system in order to circumvent sanctions or export controls.

They would sell Altamides to Albert’s firm, which would in turn resell the technology to a South African shell company, newly established by his customer for this purpose. The sales contract would state that the shell company could resell the system to an unspecified law enforcement agency. First Wap could then claim ignorance about who ended up using the system. It was, according to Goebel, a “dark grey area.” But it was “the only thing” that can “somehow protect us.”

The shell company “should not be owned by somebody who’s on the sanction list,” he cautioned, bursting into laughter.

In September, Goebel and Rudolph joined a video call with the undercover reporter posing as Albert to go through next steps on the proposal they had discussed in Prague three months earlier.

Albert pressed for a price range. “It depends on what the client chooses on the different features and the number of operators,” Goebel replied. “It can start, let’s say, minimum one million...It can get up to 15 to 20 million theoretically, if they buy all the features in there.”

Moments later, Albert revealed himself as a journalist. The call went silent.

This story is part of the Surveillance Secrets investigation, coordinated by Lighthouse Reports. It was produced in collaboration with paper trail media, ZDF, Der Spiegel, Der Standard, Tamedia, Haaretz, Tempo, KRIK, Investigace.cz, Le Monde, NRK, and IrpiMedia.

Who Was Tracked photo credits: Jennifer Bloc/Future-Image/Zuma; Balkis Press/Abaca/Zuma; Tom Williams/CQ Roll Call/Zuma; Rainer Jensen; DPA; Zuma