Ryan Gallagher **@rj_gallagher** *Mon Dec 06 07:34:00 +0000 2021*

New: Executive at Swiss Tech Company Said to Operate Secret Surveillance Operation **https://t.co/X6baoOXIQC**

The co-founder of Mitto AG, which was trusted by technology giants like Google & Twitter to deliver sensitive passwords & security codes to users, also sold a secret surveillance service to help governments spy on phones.

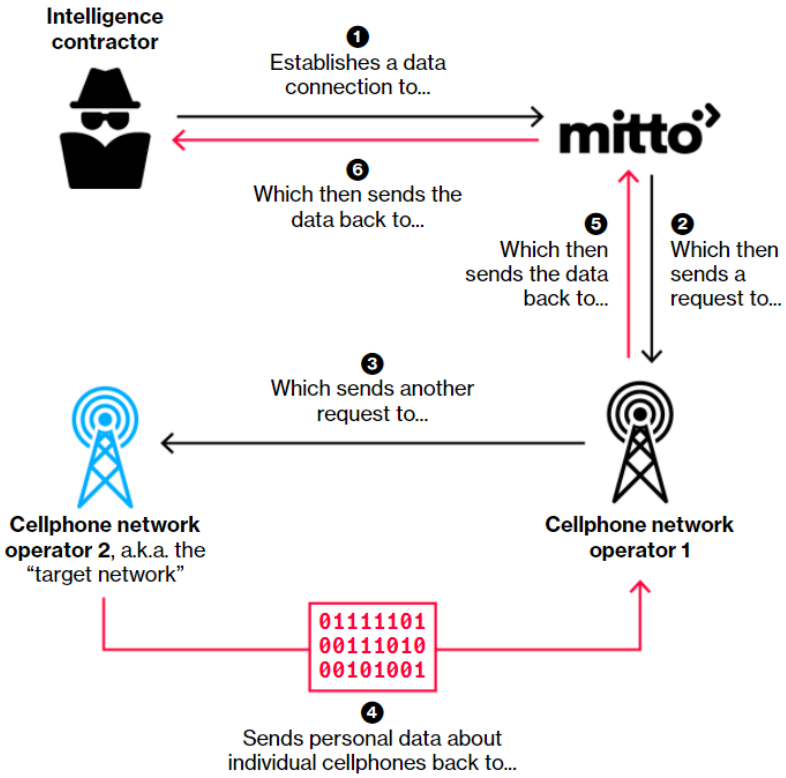
Mitto might be one of the most important companies you've never heard of. It provides automated text messages on a massive scale -- sending security codes needed to log in to online accounts as well as sales promotions & appointment reminders.

The company says it has brokered deals with telecom operators in more than 100 countries, giving it the ability to deliver text messages to billions of phones in most corners of the world.

It's attracted a host of technology giants as customers, including Google, Twitter, WhatsApp, Microsoft's LinkedIn & messaging app Telegram, in addition to China's TikTok, Tencent & Alibaba, according to Mitto documents & former employees.

But our investigation, carried out in collaboration w/ **@TBIJ**, indicates the company's co-founder & chief operating officer, Ilja Gorelik, was also providing another service: selling access to Mitto's networks to secretly locate people via their mobile phones.

The alleged venture involved exploiting weaknesses in a telecom protocol known as SS7, or Signaling System 7, a sort of switchboard for the global telecoms industry. **https://t.co/OaHBksYbtr**



People familiar with Gorelik's alleged activities said he provided surveillance services to multiple companies, including Cyprus-based TRG Research & Development.

TRG sells government agencies a system called "Intellectus" that can be used to track phone locations, monitor call & text-message records & identify people's connections on Facebook.

Former TRG employees said there was virtually no oversight of alleged surveillance carried out using Mitto's systems, creating potential opportunities for misuse.

TRG denied the allegations & said the company has never had a "commercial relationship" with Mitto & hasn't worked with Gorelik. "If anyone within TRG or Mitto has had such relationships, it is a personal relationship & is not related to TRG."

Mitto's Gorelik also told some colleagues that he had connections to a national spy agency in the Middle East & was helping that country's defense ministry track people's locations.

In one incident in November 2019, a phone number associated with a senior U.S. State Department official was targeted in 2019 for surveillance through the use of Mitto's systems, according to a cybersecurity analyst familiar with the incident & documents we reviewed.

Mitto's system was detected engaging in similar activity on dozens of other occasions globally, according to the analyst & the documents.

The revelations are "troubling" & highlight a "huge problem," said **@MarietjeSchaake**, international policy director at **@StanfordCyber**.

"The biggest technology companies that provide critical services are blindly trusting players in this ecosystem who cannot be trusted," said Schaake. "It's dangerous for human rights. It's dangerous for trust in an information society. And it's dangerous for trust in companies."

Mitto told us it had no involvement in a surveillance business & had launched an internal investigation "to determine if our technology & business has been compromised." Mitto would "take corrective action if necessary," a spokesperson said. Gorelik didn't respond to questions.

Read the full story here -- lots more detail: **https://t.co/X6baoOXlQC**

Much gratitude to **@cr0ft0n** & all at **@TBIJ** for their partnership on this project, which took a lot of work to put together. Collaborative journalism gets results ■

Huge thanks also to the many sources who helped us piece it all together -- you were vital.

If you have more information about Mitto, Gorelik & the alleged secret surveillance service he was operating, I'd love to hear from you & can offer confidentiality: **https://t.co/ZJB2GzXyzk**

UPDATE: Switzerland's federal data protection & information commissioner has just announced it's opened a "preliminary investigation" into Mitto after our story on Monday. More details to follow.

New: Swiss federal commissioner opens investigation into Mitto co-founder's alleged role providing secret surveillance service that helped governments monitor mobile phones: **https://t.co/rUi5tLFlyK**

Other developments:
- Swiss privacy lawyer says Mitto & co-founder Gorelik may have violated criminal law
- Swiss attorney general's office says it's "noted the media reports", won't comment on whether it's opening criminal probe
https://t.co/rUi5tLFlyK

NEW: Mitto Tells Clients That Co-Founder Departed After Allegations of Phone Spying **https://t.co/S2jkrIg8CW**

Mitto has informed at least two of its clients in recent days that co-founder & chief operating officer Ilja Gorelik is no longer working with the company, according to three people with knowledge of those discussions.

The development comes after we reported this last week, in partnership with **@TBIJ**:
https://t.co/M8nv9QmyeB

It's not known whether Gorelik's status at the company has changed on a permanent or temporary basis, nor is it clear if Gorelik left of his own accord.

Last week CEO Andrea Giacomini told staff in an email: "Swift actions have been taken, & we are committed to ensuring the health and wellness of our brand and our organization."

In addition, we obtained a document showing mobile network trade organisation GSMA is concerned about security weaknesses linked to the telecom protocol SS7, which it says can be used to "hide malicious or illegal activities & its true source".

SS7 is known to contain flaws that can be abused to track phones or intercept calls and messages.

The alleged surveillance service Gorelik sold involved exploiting weaknesses in SS7.

Critics contend that the mobile industry has known of these abuses for years, but has been too slow to respond.

“The lack of regulation & accountability has brought unnecessary privacy & security risks to mobile users across the globe," said Gary Miller, mobile security researcher at **@CitizenLab**. **https://t.co/S2jkrIg8CW**