TO: Human Rights Watch

This is in response to your letter of Aug. 3, 2015 regarding Hacking Team's relationship with the government of Ethiopia. Today Ethiopia is not a client of Hacking Team. The company suspended the relationship last year and terminated all relations with Ethiopia earlier this year.

Of course, Hacking Team is the victim of a criminal attack that resulted in the theft and publication of many documents and company proprietary information online in violation of the laws of Italy and all other countries. Yet the leaked information is partial, and it does not include a record of phone calls or discussions held during internal meetings at the company.

However, now that this stolen information is publicly available, Hacking Team believes that the record demonstrates that the company followed all laws and regulations as well as its own Customer Policy statement published in 2013. That policy is that when Hacking Team becomes aware of allegations of misuse of its software, it investigates to determine the facts and then may suspend the client.

Hacking Team software is operated by the client, not by Hacking Team, and the subjects of surveillance, the information gathered and the reasons for the surveillance in the first place are not available to Hacking Team.

However, Hacking Team requires clients to affirm in their contract with the company that the client will use the technology not for military purposes and only in accordance with the law.

In this case, when allegations by Citizen Lab arose in early 2014 that Ethiopia was misusing Hacking Team software, the company began an investigation and a review of the facts.

Citizen Lab alleged that the client attempted to initiate surveillance against a person identified as a 'journalist.' There was no evidence that surveillance actually took place.

The first step by Hacking Team was to interrogate the client, the Ethiopian Information Network Security Agency (INSA). Ethiopia claimed that the subject was not a journalist, but an opponent of the government that the agency had reason to believe posed a threat of violence.

Although the investigation of the facts was inconclusive, there were several within the

company who argued that irrespective of the reasons for this particular surveillance attempt, the Ethiopian investigators were inept, and the relationship with the client should be suspended for that reason alone.

As the record shows, the company decision was to suspend support the client even though the allegations by Citizen Lab were still unconfirmed.

Although Ethiopia was suspended, a contract remained in place and Hacking Team could not demonstrate violations of the contract. So discussion continued within the company about what to do about the client.

Ultimately the relationship with Ethiopia was terminated.

So the facts are these:

- Hacking Team did investigate the allegations of Citizen Lab in accordance with company policies.
- Even though there was no evidence that any surveillance actuality took place, and even though the Ethiopian client argued the attempt to surveil the suspect was justified, nonetheless, Hacking Team suspended the client in the fall of 2014.
- Ethiopia is no longer a client of the company and all relationship with Ethiopia has ended.

Finally, it is important to note that, at the time of the sale of Hacking Team technology to Ethiopia in 2011 and continuing throughout the period of the relationship, the country was never under embargo, and there are currently no restrictions on sales to Ethiopia.

Hacking Team