14 August 2015

To Human Rights Watch:

Human Rights Watch accuses Hacking Team of a "striking lack of concern about how its business could damage dissenting and independent voices" in Ethiopia. On the contrary, the facts show that the company investigated and then severed its business relationship with Ethiopia after such concerns were raised by Human Rights Watch and another group.

The very emails that Human Rights Watch relies upon to support its mistaken view actually show a broad company consideration of how to respond to allegations that the Ethiopian client used Hacking Team's software in an effort to surveil two opponents of the government.

A fair reading of the record now available thanks to stolen documents and emails posted online shows that Hacking Team did what it could to ascertain the facts of the case. Though that investigation proved somewhat inconclusive, nonetheless, Hacking Team suspended its support for the client's software in 2014 and ultimately broke off all business relationship with the client in early 2015.

Had Human Rights Watch spent as much time searching for examples of how Hacking Team software has been used effectively to fight crime in countries around the world, examples would be easy to find. For instance, this summer, Italian authorities have reported in public hearings that the technology was critical in a number of cases brought against criminals and terrorist groups. Many other law enforcement leaders have cited the need for tools to bypass what is now almost universal encryption of communications on mobile devices or the Web.

Privacy is certainly a value for all of us but so is the right of us all to be protected from crime.

Human Rights Watch often focuses on genuine cases of human rights abuse, and we are grateful for that work. However, the cause is not helped by attacking a company that has acted entirely within the law and which provides important crime-fighting tools to law enforcement around the world.

David Vincenzetti
CEO,Hacking Team