]HackingTeam[

Customer Policy

Since we founded Hacking Team, we have understood the power of our software in law enforcement and intelligence investigations. We also understand the potential for abuse of the surveillance technologies that we produce, and so we take a number of precautions to limit the potential for that abuse.

We provide our software only to governments or government agencies. We do not sell products to individuals or private businesses. We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN.

We review potential customers before a sale to determine whether or not there is objective evidence or credible concerns that Hacking Team technology provided to the customer will be used to facilitate human rights violations. We fully comply with dual use and export controls called for in the nineteenth plenary meeting of the Wassenaar Arrangement.

Moreover, in HT contracts, we require customers to abide by applicable law. We reserve the right in our contracts to suspend support for our software if we find terms of our contracts are violated. If we suspend support for HT technology, the product soon becomes useless.

We will refuse to provide or we will stop supporting our technologies to governments or government agencies that:

- We believe have used HT technology to facilitate gross human rights abuses.
- Who refuse to agree to or comply with provisions in our contracts that describe intended use of HT software, or who refuse to sign contracts that include requirements that HT software be used lawfully.
- Who refuse to accept auditing features built into HT software that allow administrators to monitor how the system is being used.

HT policies and procedures are consistent with the U.S. Know Your Customer guidelines. We conduct ongoing employee training to assure that employees know and understand the provisions of these guidelines.
Should we discover “red flags” described in these guidelines while negotiating a sale, we will conduct a detailed inquiry into the matter and raise the issue with the potential customer. If the “red flags” cannot be reasonably explained or justified, we may suspend the transaction.

Our review will include:

- Statements made by the potential customer either to HT or elsewhere that reflect the potential for abuse.
- The potential customer's laws, regulations and practices regarding surveillance including due process requirements.
- Credible government or non-government reports reflecting that a potential customer could use surveillance technologies to facilitate human rights abuses.

Hacking Team encourages anyone with information about apparent misuse or abuse of our systems and solutions to promptly report that information to us at info@hackingteam.com.

Hacking Team has established a process of monitoring news media, activist community blogs and other Internet communication, and other available sources for expressed concerns about human rights abuses by customers or potential customers. Should questions be raised about the possible abuse of HT software in human rights cases, HT will investigate to determine the facts to the extent possible. If we believe one of our customers may be involved in an abuse of HT software, we will contact the customer as part of this investigation. Based on the results of such an investigation, HT will take appropriate action.