

350 Fifth Avenue, 34<sup>th</sup> Floor  
New York, NY 10118-3299  
Tel: +1-212-290-4700  
Fax: +1-212-736-1300; 917-591-3452

Kenneth Roth, *Executive Director*

**DEPUTY EXECUTIVE DIRECTORS**

Michele Alexander, *Development and Global Initiatives*  
Carroll Bogert, *External Relations*  
Iain Levine, *Program*  
Chuck Lustig, *Operations*

Dinah PoKempner, *General Counsel*  
James Ross, *Legal and Policy Director*

**DIVISION AND PROGRAM DIRECTORS**

Brad Adams, *Asia*  
Daniel Bekele, *Africa*  
Alison Parker, *United States*  
José Miguel Vivanco, *Americas*  
Sarah Leah Whitson, *Middle East and North Africa*  
Hugh Williamson, *Europe and Central Asia*

Joseph Amon, *Health and Human Rights*  
Shantha Rau Barriga, *Disability Rights*  
Peter Bouckaert, *Emergencies*  
Zama Coursen-Neff, *Children's Rights*  
Richard Dicker, *International Justice*  
Bill Frelick, *Refugee*  
Arvind Ganesan, *Business and Human Rights*  
Liesl Gertholtz, *Women's Rights*  
Steve Goose, *Arms*  
Graeme Reid, *Lesbian, Gay, Bisexual, and Transgender Rights*

**ADVOCACY DIRECTORS**

Philippe Boloipon, *United Nations, New York*  
Maria Laura Canineu, *Brazil*  
Kanae Doi, *Japan*  
Jean-Marie Fardeau, *France*  
Meenakshi Ganguly, *South Asia*  
Tiseke Kasambala, *Southern Africa*  
Lotte Leicht, *European Union*  
Sarah Margon, *Washington DC*  
David Mepham, *United Kingdom*  
Wenzel Michalski, *Germany*  
Elaine Pearson, *Australia*  
Juliette de Rivero, *United Nations, Geneva*

**BOARD OF DIRECTORS**

Hassan Elmasry, *Co-Chair*  
Joel Motley, *Co-Chair*  
Wendy Keys, *Vice-Chair*  
Susan Manilow, *Vice-Chair*  
Jean-Louis Servan-Schreiber, *Vice-Chair*  
Sid Sheinberg, *Vice-Chair*  
John J. Studzinski, *Vice-Chair*  
Michael G. Fisch, *Treasurer*  
Bruce Rabb, *Secretary*  
Karen Ackman  
Jorge Castañeda  
Tony Elliott  
Michael E. Gellert  
Hina Jilani  
Betsy Karel  
Robert Kissane  
Kimberly Marteau Emerson  
Oki Matsumoto  
Barry Meyer  
Aoife O'Brien  
Joan R. Platt  
Amy Rao  
Neil Rimer  
Victoria Riskin  
Graham Robeson  
Shelley Rubin  
Kevin P. Ryan  
Ambassador Robin Sanders  
Javier Solana  
Siri Stolt-Nielsen  
Darian W. Swig  
John R. Taylor  
Amy Towers  
Marie Warburg  
Catherine Zennström

February 25, 2015

Mr. David Vincenzetti and Mr. Valeriano Bedeschi  
Hacking Team (HT S.r.l.)  
Via della Moscova n.13  
20121 - Milano  
Italy

Cc: Mr. Eric Rabe

**Re: Update on Sale and Use of Hacking Team Solutions in Ethiopia**

Dear Mr. David Vincenzetti and Mr. Valeriano Bedeschi:

Human Rights Watch is an independent international organization that monitors human rights in more than 90 countries around the world. I am writing to request your input and perspective regarding follow-up to our March 2014 report, *They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia*, which documents Ethiopian government human rights violations facilitated by abusive digital surveillance.

The report describes several attempts to target and infect the computers of several Ethiopian Satellite Television Service (ESAT) employees with spyware that appeared to be Hacking Team's Remote Control System (RCS). ESAT is an independent, diaspora-run television station based in Amsterdam. The report also documents how the Ethiopian government has used abusive surveillance to target journalists and opposition groups to silence independent voices.

We have learned through updated research conducted by Citizen Lab that several US-based ESAT employees were targeted again in November and December 2014 with spyware that matches previously established characteristics of Hacking Team's RCS. Citizen Lab's research traced the attack to Internet Protocol addresses linked to Ethio Telecom and elements of the attack also appear to connect it to earlier 2013 attacks documented in our report.

The new information disclosed to us from Citizen Lab also found that the RCS spyware used in the attacks against ESAT was updated as recently as



HRW.org

December 2014. On November 19, 2014, security researcher Claudio Guarnieri publicly released a tool called Detekt, which can be used to scan computers for Hacking Team RCS and other spyware.<sup>1</sup> **Citizen Lab's testing determined that Detekt was able to successfully** recognize the version of RCS used in the November 2014 attack, but not the version used in the December 2014 attack. This appears to indicate that the software had been updated. Citizen Lab plans to publish these new findings.

We are concerned that, if accurate, these findings indicate that Hacking Team has continued to sell, support, or update intrusive surveillance solutions to the Ethiopian government. These actions may have continued despite clear and credible evidence from a range of media reports and research by independent human rights organizations in the last year that has documented the **Ethiopian government's** established record of serious violations, often facilitated by misuse of surveillance powers.

**We have documented how abusive surveillance practices and misuse of Ethiopia's deeply flawed anti-terrorism law** have been used to silence independent voices inside and outside Ethiopia.<sup>2</sup> We are particularly concerned because the environment for media freedom, freedom of expression, and independent civil society has worsened in 2014, ahead of the May 2015 general elections in the country.<sup>3</sup> In the past year, six privately owned print media publications closed after harassment, at least 22 journalists, bloggers, and publishers were criminally charged, and more than 30 journalists fled the country in fear of being arrested under repressive laws.

The government has also gone further to thwart and discourage individuals from adopting surveillance counter-measures to protect their privacy and security. In 2014, seven bloggers from Zone 9, who write on current events in Ethiopia, along with three journalists, were charged under **the country's abusive** antiterrorism law. Among the evidence the prosecution cited was the digital security and encryption training that the bloggers took to learn to shield their communications and avoid reprisals. These arrests have had a broad chilling effect on freedom of expression in Ethiopia.

Given this context, we want to better understand the steps Hacking Team has taken to address any abuse of its products and services by the Ethiopian government. We would appreciate any

---

<sup>1</sup> Detekt, "Detekt: Resist Surveillance," undated, <https://resistsurveillance.org> (accessed February 25, 2015); Eva Galperin, "Detekt: A New Malware Detection Tool That Can Expose Illegitimate State Surveillance," post to Deeplinks (Blog), November 20, 2014, <https://www.eff.org/deeplinks/2014/11/detekt-new-malware-detection-tool-can-expose-illegitimate-state-surveillance> (accessed February 25, 2015).

<sup>2</sup> Human Rights Watch, "*They Know Everything We Do*": *Telecom and Internet Surveillance in Ethiopia*, March 25, 2014, <http://www.hrw.org/reports/2014/03/25/they-know-everything-we-do>.

<sup>3</sup> Human Rights Watch, "*Journalism Is Not a Crime*": *Violations of Media Freedoms in Ethiopia*, January 22, 2015, <http://www.hrw.org/reports/2015/01/21/journalism-not-crime>.

information or comment you may have on the information Citizen Lab has provided to us as described above to inform our response, along with specific replies to the following questions. This will greatly assist our understanding of Hacking Team, the products and solutions it offers, its approach to human rights risk, and how it has responded to credible reports of illegal surveillance and other human rights abuses against Ethiopians both inside and outside of Ethiopia.

1. **Hacking Team’s Customer Policy states that it monitors news media and other sources for reports of potential human rights abuses by existing or potential Hacking Team customers, and invites disclosure of information about “apparent misuse or abuse of [the company’s] systems and solutions.” The policy also states that “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.”**<sup>4</sup>

*To what extent has Hacking Team investigated Ethiopia’s alleged abuse of surveillance technologies, including Hacking Team’s systems, reported in our March 2014 report, as well as the work done by Citizen Lab in the last year? What was the result of any investigation and what actions were taken?*

2. Hacking Team previously stated to Human Rights Watch **that, “we expect our clients to behave responsibly and within the law as it applies to them” and that the firm will suspend support for its technology if it believes the government customer has used it “to facilitate gross human rights abuses” or “who refuse to agree to or comply with provisions in [the company’s] contracts that describe intended use of HT software.”**<sup>5</sup> Hacking Team has also stated it has previously suspended support for their product, in which case **the “product soon becomes useless.”**<sup>6</sup>

*What are the allowable end uses described in Hacking Team contracts? Have these allowable uses been violated by the Ethiopian government, given evidence presented in our human rights reporting in Ethiopia and evidence presented by Citizen Lab?*

*Has Hacking Team ever suspended support for any products or services in Ethiopia? What steps, if any, has Hacking Team taken to address human rights harm allegedly linked to its products or services in Ethiopia?*

---

<sup>4</sup> Hacking Team, “Customer Policy,” 2013, <http://www.hackingteam.it/index.php/customer-policy> (accessed February 25, 2015).

<sup>5</sup> Human Rights Watch, “*They Know Everything We Do*”; Hacking Team, “Customer Policy.”

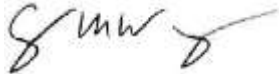
<sup>6</sup> Hacking Team, “Customer Policy.”

3. Hacking Team’s Customer Policy states that through contract, the company “requires customers to abide by applicable law” and that Hacking Team will not sell or provide support to governments who “refuse to sign contracts that include requirements that [Hacking Team] software be used lawfully.”<sup>7</sup>

*Please describe the specific laws (or categories of law) Hacking Team requires customers to abide by. To what extent have you raised Ethiopia’s obligations under international human rights treaties to protect freedom of expression, the right to privacy, media freedom, and other rights with government customers? How do you evaluate lawful use where local law is inconsistent with the government’s international human rights obligations?*

Thank you for your consideration and we look forward to your responses to our inquiries. We would also welcome the opportunity to discuss these issues with you further. Should you have any questions, please do not hesitate to contact me.

Sincerely,



Cynthia Wong

Senior Internet Researcher, Business and Human Rights Program  
Human Rights Watch

---

<sup>7</sup> Ibid.