Response from Sandvine

The Business & Human Rights Resource Centre invited Sandvine to respond to allegations that deep packet inspection technology produced by Sandvine has been used to facilitate human rights violations by repressive governments, including censorship through a recent internet shutdown in Belarus.

- "U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet", 11 September 2020, *Bloomberg*
- "Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus", 3 September 2020, *Access Now*
- "Belarusian Officials Shut Down Internet With Technology Made by U.S. Firm", 28 August 2020, *Bloomberg*

On 15 September 2020, Sandvine sent the following response:

"Sandvine takes human rights abuses very seriously. We also abhor the use of technology to suppress the free flow of information resulting in human rights violations. That's why we launched an investigation into the situation in Belarus.

Sadly, preliminary results of our investigation indicate that custom code was developed and inserted into Sandvine's products to thwart the free flow of information during the Belarus election. This is a human rights violation and it has triggered the automatic termination of our end user license agreement.

Sandvine will no longer sell our products in Belarus. Our end user license agreement explicitly prohibits actions that supports or enables the commission of individual human rights violations.

Sandvine did not violate any U.S. or other applicable export control laws or sanctions.

From a technology standpoint, we are exploring ways to enhance our products to reduce the risk of misuse.

From a customer standpoint, Sandvine is strengthening its already vigorous process of reviewing new customers to assess the risk that our products might be used by them in a manner detrimental to human rights. Information about our company's ethics policy is available at http://www.sandvine.com/company/corporate-ethics.

About the technology:

URL blocking and filtering technology is incorporated into virtually all network infrastructure, security and firewall equipment.

URL blocking and filtering protects networks and subscribers against illicit and illegal activities, such as child pornography, human trafficking, terrorism, and the spread of malware.

Many of the world's largest communications infrastructure and security companies manufacture and sell URL blocking and filtering technology for the purpose of protecting the public from illegal and illicit activities.

URL blocking and filtering technology is not government-regulated and is commonplace in the U.S., Canada, and other Western countries.”