Dear Business & Human Rights Centre:

On December 22, 2025, you invited AppLogic Networks to respond by January 23, 2026 to an investor guide that you plan to publish concerning risks relating to certain technologies. We appreciate the opportunity to engage on this important topic and provide the following in response.

In your draft report, you reference a case study concerning Sandvine Corporation. We note that you referred to the company as "AppLogic Networks (formerly Sandvine)," but we want to emphasize that AppLogic Networks is a new entity, entirely distinct from its predecessor Sandvine Corporation (see Sandvine emerges as AppLogic Networks), and the conduct you describe relates only to Sandvine, not to AppLogic Networks.

The differences between AppLogic Networks and Sandvine should not be oversimplified as a mere name change. AppLogic Networks does business in democracies, which means that we do not engage in business with governments and third parties in countries that are deemed authoritarian by leading independent global indices such as The Economist, Democracy Index, and Freedom on the Net Report.

As your report recognizes, risk mitigation processes alone have proven to be insufficient to prevent product misuse in this industry. AppLogic Networks is the only networking vendor in the world that has gone further by choosing to do business in democracies, rather than relying on risk mitigation processes alone to reduce the risk of product misuse.

AppLogic Networks' approach recognizes that internet-related technologies can be used responsibly, including to ensure the effective operability of the internet, but these same technologies can also be misused in ways that violate human rights. We believe the most effective way to prevent, detect, and minimize the potential misuse of our products is to simply not sell these technological capabilities in non-democratic countries and to apply risk-based human rights due diligence in the jurisdictions where we operate.

The technological capabilities your report references are not unconventional or fringe. In fact, they are typical capabilities regularly used to facilitate the safe and efficient operation of public and private networks around the world. These capabilities, such as blocking IPs, ports, sites, and applications, are functions that all firewalls, proxies, routers, and thousands of networking products are designed to perform. They also include standard capabilities such as redirecting traffic from one IP or site to another or logging access in an IP database for some or all IP records. All of these capabilities are standard by Internet Engineering Task Force (IETF) constructs, but, as with many other tools in both the internet and physical spheres, they have the possibility of being misused by bad actors.

Your report also appears to conflate technologies that redirect network traffic with deep packet inspection (DPI) technologies. However, redirect capable technology is not an intrinsic capability of DPI technology; rather, it is an industry standard capability that is

implemented on most IP middleboxes.[1] In particular, your report suggests that DPI technologies by their very nature are nefarious. This suggestion lacks important nuance. DPI, like many other networking tools, can be misused. There are numerous lawful and legitimate applications of DPI implemented by public and private networks around the world, including critically important protective commercial applications such as intrusion prevention, malware blocking, traffic management (to prioritize critical data flows and improve quality of service), policy enforcement (malicious content filtering and preventing data leaks), and targeted advertising.

AppLogic Networks' mission is to make the Internet available to everyone, enhance the quality of their network experience, and champion digital human rights. Accordingly, we have committed to a democracy-oriented go-to-market strategy to reduce the risk of product misuse that infringes upon human rights. AppLogic Networks also does not sell hardware, nor has it ever provided spyware or worked with spyware vendors.

Furthermore, AppLogic Networks has taken significant steps to improve its human rights due diligence program to prevent, detect, and continuously improve efforts to mitigate human rights risks relating to its business, including those relating to potential third party misuse of its products (*see* AppLogic Networks: Putting Business Integrity into Action and What We're Doing and Why It Matters). These actions include:

1	Dedicated and independent Human Rights Committee, reporting to the Board of Directors
2	Independent Human Rights Senior Advisor, reporting directly to the ALN Board of Directors
3	Dedicated Chief Ethics and Compliance Officer, reporting directly to the CEO
4	Public commitment to respect human rights, mitigate risks of potential third party product misuse to violate human rights, and take action to remediate identified third party product misuse involving ALN products
5	Conducts business in democracies and continues to conduct human rights due diligence globally
6	Public commitment to provide 1% of annual profits to one or more NGOs that protect human rights, human rights defenders, journalists, and others, and promote Internet freedom
7	Publicly available Human Rights Statement informed by the U.N. Guiding Principles (UNGPs), informed by members of civil society, NGOs, and other outside advisors, and references the International Bill of Human Rights
8	Global Human Rights Due Diligence & Risk Management Policy (HRDD Policy), informed by the UNGPs, input from civil society members, NGOs, and other outside advisors. The HRDD Policy applies globally and provides a framework for how the company mitigates salient human rights risks relating to its products

[1] See Request for Comments: RFC 3234 - Middleboxes: Taxonomy and Issues.

9	Maintains a Progressive Escalation Framework, which includes the Company's investigation practices and ability to contractually suspend, withdraw, and/or terminate services in the event of identified third party product misuse involving ALN products
10	Contractual clauses in its customer end user license agreements that require responsible use of the Company's products
11	All employees, including Company senior leadership, are required to take training regarding human rights related potential risks associated with ALN products, which includes fundamentals of corporate responsibility under the UNGPs
12	Conducts pre-sale human rights due diligence concerning certain sales opportunities, which has resulted in the Company declining certain sales opportunities
13	Monitors the risk landscape as well as indicia of potential third party product misuse involving ALN products post sale
14	Maintains an independent third-party grievance mechanism, which allows for anonymous reporting from internal and external stakeholders to manage allegations, including potential product misuse
15	Maintains an active Business Ethics Committee comprised of senior Company executives that implement the Company's HRDD Policy and evaluate human rights related risks associated the Company's products, and includes technical staff to field questions relating to product capabilities
16	Participates in multistakeholder initiatives and/or forums that prioritize respecting human rights, including by serving as an observer of the Global Network Initiative
17	Supports its legal predecessor company's (Sandvine Corporation's) periodic reports to the U.S. Government regarding its compliance with its commitments, including reporting on Sandvine's completion of its exit from over 20 non-democracies as of December 31, 2025
18	Committed to cooperate in good faith with any judicial, government, or regulatory investigations of potential product misuse involving the Company's products
19	Maintains a no retaliation policy against any person for raising a concern, reporting an issue, or critiquing the Company in good faith
20	Code of Conduct informed by the UNGPs
21	New corporate value of "Doing the Right Thing," includes doing the right thing to respect human rights and responsible business practices
22	In AppLogic Networks' products, subscriber identities are obfuscated to protect privacy. Use of subscriber identities in clear text requires a customer to secure a specific product license
23	In AppLogic Networks' products, wherever possible, functions such as the redirect capability are made apparent in the network traffic (via IP identifiers

	and headers) to provide greater visibility that an AppLogic Networks' product is being used and to identify the third-party user
24	In AppLogic Networks' products, features that may be misused such as redirect and blocking are all features which require a license and enable AppLogic Networks to be more surgical in what capabilities are sold and the manner in which our products can be used

The steps AppLogic Networks have taken to align its business operations with democratic values are rare and unprecedented in our industry.

They differentiate AppLogic Networks from others in the industry, match the company's profits with its purpose, and put business integrity into action in ways that are unique and not readily seen, duplicated, or implemented by other corporations with comparable risks and/or similar technologies.

Thank you again for the opportunity to respond and including our response in the annex to your report.

Best regards,

Carol Tate
Chief Ethics and Compliance Officer
AppLogic Networks