TECHNICAL MODEL NATIONAL RESPONSE

The Technical Model National Response is inspired by WePROTECTs Model National Response. It works to highlight that technology and digital tools must be applied by all sectors and businesses in order to ensure that a country has a comprehensive model to fight online child sexual abuse material.

1. BUSINESSES AND ORGANIZATIONS (DETECTION TOOLS)

• Detection tools identify when corporate computers and networks are used to view, distribute and download child sexual abuse material. When material is found the Police is notified.
• The signature-based detection makes it possible to find the material regardless of what source the image comes from (Such as USB, Darknet or the Open web)

2. SOCIAL MEDIA PLATFORMS AND SEARCH ENGINES (TAKEDOWN & NOTICE AND KEYWORD BLOCKING)

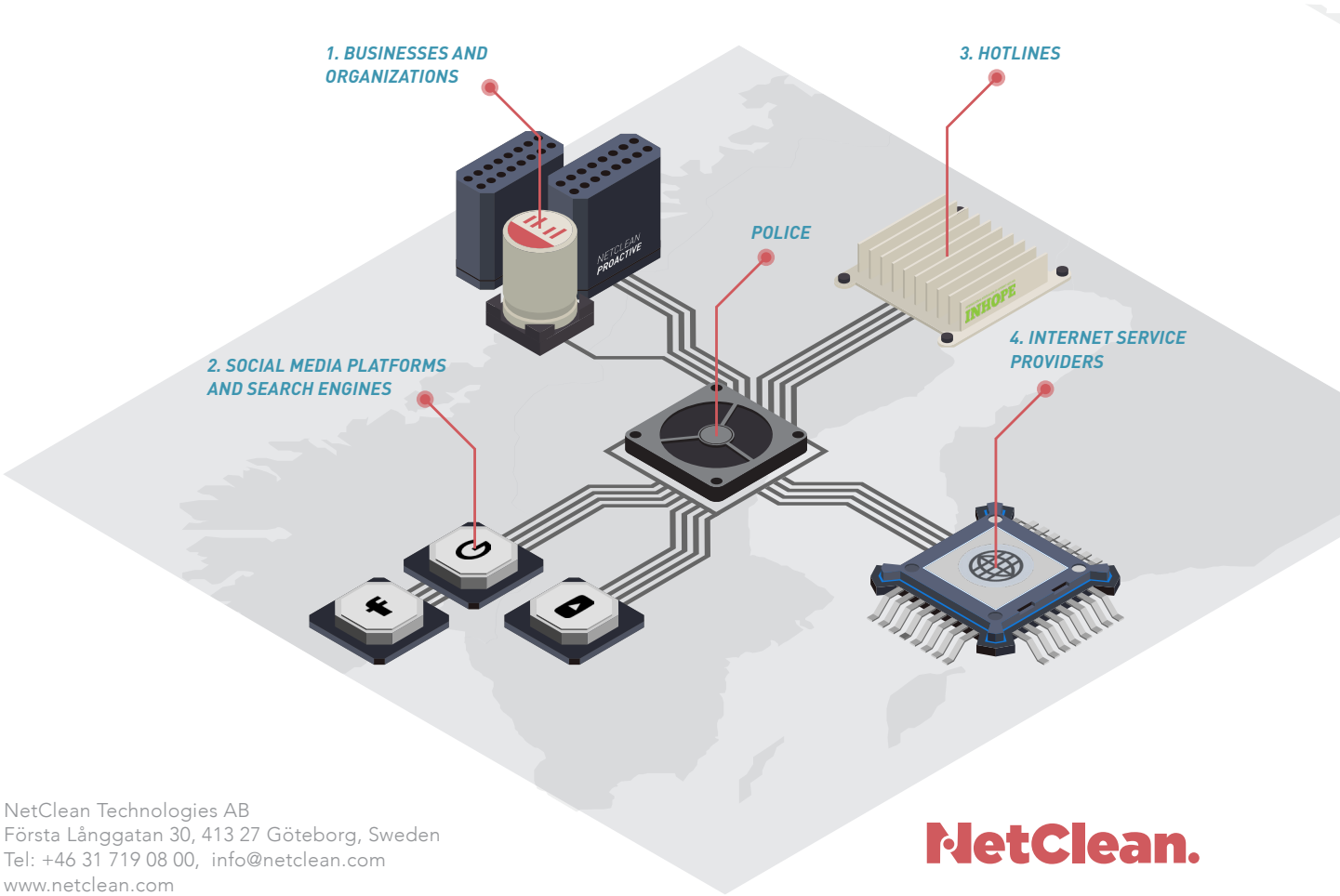
• Search engines like Google and Social media companies like Facebook, KiK, and Snapchat report material found on their platforms.
• Search engines also use tools like key word blocking on their platforms to limit access to child sexual abuse material.

3. HOTLINES (TAKEDOWN & NOTICE AND CRAWLERS)

• Hotlines, like INHOPE, receive tips from the public and use technology that result in takedown and notice.
• Automated crawlers, like Project Arachnid, detect where confirmed child sexual abuse images and videos are publicly available on the Internet. If illegal content is detected, a notice is sent to the provider hosting the content to request its removal, and it is also fed back to the police.

4. INTERNET SERVICE PROVIDERS (BLOCKING)

• ISPs block access to sites known to contain child sexual abuse material by using different blocking technologies with lists from example Interpol, IWF or the National Police.



NetClean Technologies AB
Första Långgatan 30, 413 27 Göteborg, Sweden
Tel: +46 31 719 08 00, info@netclean.com
www.netclean.com

NetClean.