



FOR IMMEDIATE RELEASE

**Internet Filtering as Part of the USA National Broadband Plan
and the American Recovery and Reinvestment Act of 2009 (i.e. the Stimulus Package)**

JACKSONVILLE, FLORIDA USA – Friday April 10, 2009 – BluePrint Data this week provided comments for the Federal Trade Commission’s (FTC) implementation of the Broadband Data Improvement Act, part of the American Recovery and Reinvestment Act of 2009 (Recovery Act). The goal of the act includes measures to modernize our nation's Internet and communications infrastructure the FCC oversees, specifically, the Broadband Technology Opportunities Program established by the Act, and the FCC creation of a National Broadband Plan. BluePrint Data’s comments relate to the necessity and cost savings of Internet Filtering as part of the broadband plan.

The Recovery Act states that the National Broadband Plan shall seek to ensure all people of the United States have access to broadband capability and shall establish benchmarks for meeting that goal. BluePrint Data believes Internet Filtering and Security is an important aspect of that goal and believe the Commission should include network technologies for Internet Filtering (i.e. Web site filtering / Parental Controls) as part of the implementation of sections 103(b) and 103(c)(1) of the Broadband Data Improvement Act

Internet Filtering technology and Parental Controls are provide by most current broadband service providers in the USA and other countries. These technologies range from network based (filtering via a proxy server or at a router or switch) to client based installations. Many residential consumers expect this type of service to be included (i.e. bundled) in their monthly access charge / fee. And some of the network services such as proxy servers¹, caching appliances and application accelerators can increase actual data transmission speeds to the end user / consumer. Actual data transmission speeds increases of 1,000% and more are possible.

Filtering illegal and harmful content is important for families and especially children whom lack the cognitive development to “process” what they may find on the Internet. This is especially true when considering viewing Internet content in public spaces or across the public airwaves (wireless broadband).

Internet Filtering can protect children from potentially harmful or illegal content that may impair...

* their moral or social development (example: content that may have a traumatizing effect)

* their sexual development (example: sexual content that may have a traumatizing effect)

- * their emotional and mental development (example: other content that may have a traumatizing effect)

It can also protect children from potentially harmful or illegal content that may instigate...

- * damage to another (rape, harassment, etc.)
- * damage to another's life (murder, terrorism, etc.)
- * damage to another's rights (racism, sabotage, theft, etc.)
- * damage to him/herself (drug abuse, gambling, meeting strangers, etc.)
- * damage to his/her life (suicide, severe drug abuse, etc.)

BluePrint Data believes some form of Internet Filtering / Parental Controls is integrally needed as part of the Broadband Data Improvement Act.

About BluePrint Data.

BluePrint Data provides its URL filter and content filtering technology, services, and products to Internet Security vendors including UTM, MSSP and SaaS, enables ISPs, telecommunication companies and carriers to filter and manage their Internet traffic and provide Internet Filtering solutions to Information Technology Solutions Providers and Value Added Resellers (VARs). BluePrint Data has the world's largest 100% human reviewed URL Filter Database covering over 800 million web pages that is combined with Internet security services to provide solutions for: Internet Security Companies, Telecom and Carriers, and Businesses and Organizations.

###

FOR MORE INFORMATION:

Bob Dahlstrom

BluePrint Data

904-647-4491

press@blueprintdata.com

Keywords:

OEM URL Filter, OEM Internet Filter, OEM Internet Security, Internet Security Attack Paradigm, Client Web Browser Attacks, Client Side Based Attacks, Internet Filtering, Internet Security, ISP, Carrier, Telecom, Telecommunications, BluePrint Data, Carrier Internet Filtering, Telecom Internet Filtering, Carrier Internet Security, Telecom Internet Security, ISP Internet Security, content filtering, content filtering software, Enterprise Internet Filtering, filter drug, filter gambling, filter hate, filter porn, filter stock, Internet Filter database, web filter database, internet Filtering, Internet Filtering Appliance, Internet Security, Internet Security Service provider, managed content filtering, malware filtering, Managed Security Service Provider, managed VPN, MSSP, managed malware filtering, malicious URL filter, OEM URL Database, OEM URL List, outsourced security, Internet Security SaaS, SaaS, Secure Computing, Software as a Service, Unified Threat Management, URL, URL Database, URL Filter, URL Filter Database, URL Filter DB, UTM, Web page filter

¹ From Wikipedia – April 9, 2009 - In computer networks, a **proxy server** is a server (a computer system or an application program) that acts as a go-between for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client's request or the server's response, and sometimes it may serve the request without contacting the specified server. In this case, it 'caches' responses from the remote server, and returns subsequent requests for the same content directly.

A proxy server has two purposes;

- * To keep machines behind it anonymous (mainly for security).
- * To speed up access to a resource (via caching). It is commonly used to cache web pages from a web server.

http://en.wikipedia.org/wiki/Proxy_server

Caching Appliances and **Application Accelerators** work similar to proxy servers with the purpose of increasing the response speed to resources including web site content and multimedia formats such as video.