Association for Information Systems
AIS Electronic Library (AISeL)

All Sprouts Content Sprouts

7-24-2010

# A Concise Study of Web Filtering

M. Tariq Banday
*University of Kashmir*, sgrmtb@yahoo.com

Nisar A. Shah
*University of Kashmir*, nassgr@yahoo.com

## Recommended Citation

Banday, M. Tariq and Shah, Nisar A., " A Concise Study of Web Filtering" (2010). *All Sprouts Content*. 352.
http://aisel.aisnet.org/sprouts_all/352

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

# A Concise Study of Web Filtering

M. Tariq Banday
University of Kashmir, India

Nisar A. Shah
University of Kashmir, India

## Abstract

Cybercriminals are constantly developing techniques to infect computers by embedding malicious code on innocent websites and luring victims to them. To prevent data loss in a mobile connected world, corporations are employing a variety of techniques. These include filters, anti-virus software, encryption and firewalls, access control, written policies and improved employee training. This paper conducts a concise study of web filtering vis-à-vis their installed positions, deployment layers, employed filter technologies and comparison between Web Filters that are in place in Canada, United Kingdom, and China.

**Keywords:** Web Filtering, Filter Deployment, Filter Operating Layers, Rating Filters, Blacklisting, Keyword Matching, Dynamic Filtering.

**Permanent URL:** http://sprouts.aisnet.org/10-31

**Reference:** Banday M.T., Shah N.A. (2010). "A Concise Study of Web Filtering," . *Sprouts: Working Papers on Information Systems*, 10(31). http://sprouts.aisnet.org/10-31

# A Concise Study of Web Filtering

**M. Tariq Banday, Nisar. A. Shah**

*P.G. Department of Electronics and Instrumentation Technology,*
*University of Kashmir, Srinagar - 6, India*
*E-mail: sgrmtb@kashmiruniversity.ac.in*

## Abstract

Cybercriminals are constantly developing techniques to infect computers by embedding malicious code on innocent websites and luring victims to them. To prevent data loss in a mobile connected world, corporations are employing a variety of techniques. These include filters, anti-virus software, encryption and firewalls, access control, written policies and improved employee training. This paper conducts a concise study of web filtering vis-à-vis their installed positions, deployment layers, employed filter technologies and comparison between Web Filters that are in place in Canada, United Kingdom, and China.

## Keywords

Web Filtering, Filter Deployment, Filter Operating Layers, Rating Filters, Blacklisting, Keyword Matching, Dynamic Filtering.

## Introduction

Web filtering is a class of content filtering techniques [1] used by corporations and home users as a part of Internet firewall to determine whether incoming data is harmful to the network or outgoing data includes any intellectual property. The filter checks every Web page against a set of predefined rules and blocks harmful and objectionable data like pornographic material, spyware, viruses, etc. from entering the network or the home computer.

Web Filtering guarantees manageable Internet access by reducing the unnecessary use of network resources, increasing work productivity, decreasing risks of Internet abuse, and decreasing security and legal risks.

More than forty Western and non-Western countries including Saudi Arabia, Iran, Norway, Sweden, Denmark, UK, and Netherlands are using Web filters to block Websites considered to be inappropriate.

## Filter Deployment

A Web Filter can be installed at various places in the Network and may operate at various levels of the OSI Model as depicted in figure 1. The legends1 through 5 denote the place of filter as explained in the below paragraphs. The customization options, Performance of the filter and Security provided depend greatly on the place of the deployment [2, 3].

1. ***At National/Country Level:*** The Filter is deployed between the national Internet Backbone and the country network. Several nations including China and Saudi Arabia have implemented filters at National Level. Filter Configuration is wholly determined by the Governmental. Users have no control over filter customization, its performance and thus security provided by the filter is determined by the policy of the Government.

2. ***At Organizational Level:*** The Filter is deployed between the Organizational Network and the Internet Gateway. All users of this Gateway Server e.g. all employees of the Organization are provided filtered Internet Content. The KU Gateway installed at http://192.168.81.251:8090/corporate/servlet/CyberoamHTTPClient is an example of Organizational Level Filtering. The filter is customizable by the Organizations Web Administrators keeping into consideration the Organizational policy regarding what is appropriate and what is not for the organization. Organizations besides providing filtered content also can limit the durations of use of the Internet.

3. ***At Internet Server Provider:*** The Filter is installed at the ISP Gateway and provides filtered content to all its customers. Informal Government pressures in Canada and UK led major ISPs to voluntarily institute filtering to block inadequate access to child pornography and child abuse material. Courts in France, Belgium and Germany have ordered ISPs to block hate speeches and the illegal peer to peer file shearing of copyright protection material. As per our knowledge no ISP in India provides filtered content to its customers.

4. ***At Individual Level:*** The Filter is installed at the local computer or workstation. The Filter may be part of a Firewall, Antivirus package, or through some other similar system like Content Advisor, Parental Control, etc.

5. ***At Third-Party***: The Filtering service is provided by a trusted third party vendor through its Security Operation Canters (SOCs). The customers send their Web Traffic through these SOCs by proxying. ScanSafe and WebSense are the examples of such Third-Party

Vendors. Although suitable for all kinds of organizations and users, this service is limited to small and medium organizations but offers filtering at any level of an organization.

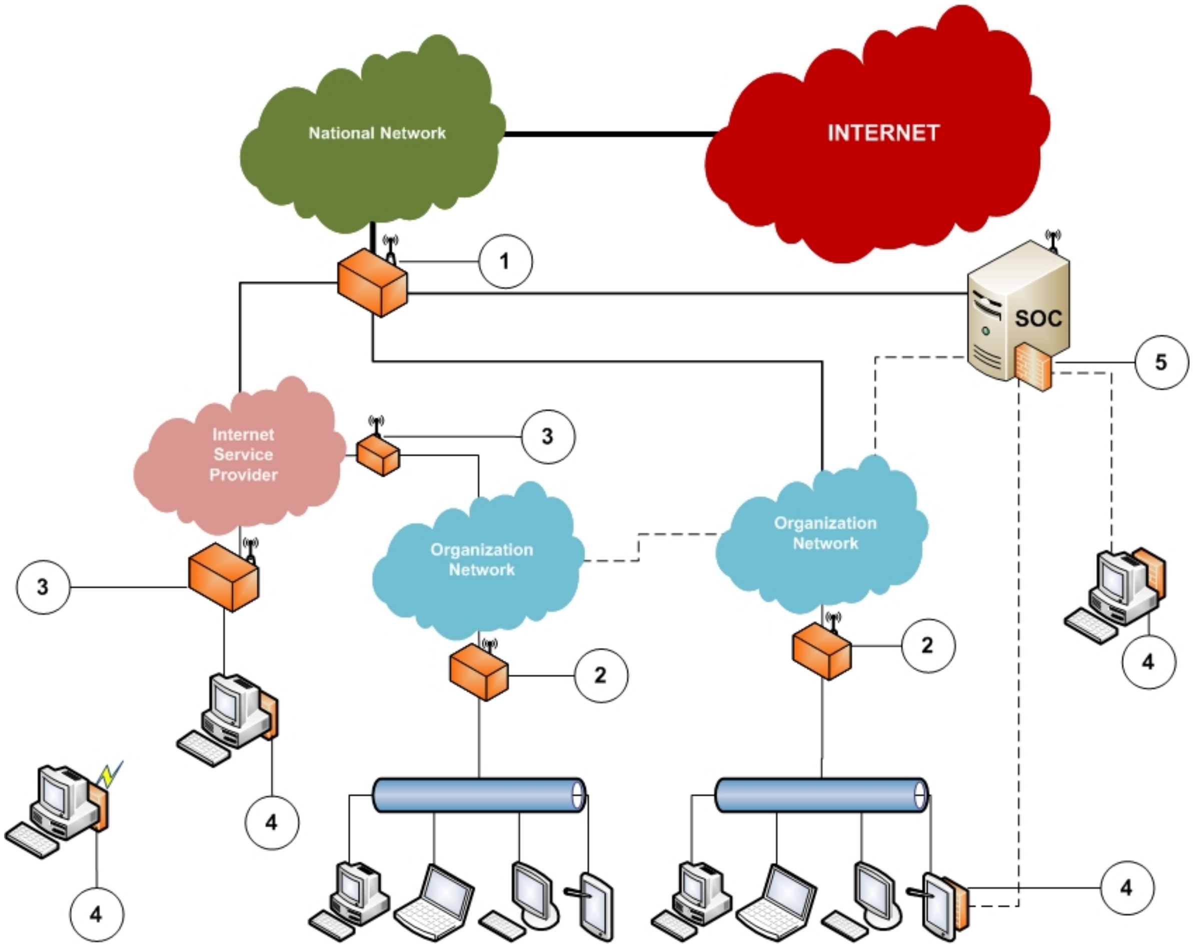

***Figure 1:*** *Filter Deployment*

## Filter Operating Layers

The Filter installed at various places in the network may operate at either layer 3 called ***Network Layer*** or layer 4 called ***Transport Layer*** or at Layer 7 called ***Application Layer*** of the OSI Networking Model. Filters installed at Layers 3 and 4 are referred to as Network Layer Filters and those installed at Layer 7 are called Application Layer Filters.

1. **Layer 3** of the ***OSI*** model is responsible for logical addressing and routing of data using protocols like IP. The packet contains source and destination addresses which can be used to block the transmission of the packet based on some defined rules of the filter.

2. **Layer 4** of OSI model is responsible for formatting and transporting data using protocols like TCP and UDP. The packet at this layer contains source and destination addresses besides containing information about the type of network traffic thus enabling blockage of traffic from certain address meant for a particular application.

3. **Layer 7** of the OSI model is responsible for data analysis before sending it to a particular application. At this layer packets are assembled and thus inspection of the data arriving for a particular application can be undertaken by performing deep inspection for the content filtering. Application Proxy firewall operates at this layer of the OSI model.

| | |
|---|---|
| **Application Layer**<br>**Layer 7** | • *Enables user to accept to access the network. Provides user Interfaces and support to services like email, WWW, FTP, remote Login, etc.* ***Gateway*** *Operates at this Layer. Addressing varies on the basis of service e.g. email addresses, URL Addresses, FTP connection addresss, etc.* |
| **Presentation Layer**<br>**Layer 6** | • *Handles the Systax and Sementics of the information exchanged between two applications. Provides translation of Syntax between different systems, encryption, decryption and compression.* |
| **Session Layer**<br>**Layer 5** | • *Acts as a network dialog controller. Establishes, maintains and synchronizes the interaction between two systems.. Provides Dialog Control and Dialog Seperation Services.* |
| **Transport Layer**<br>**Layer 4** | • *Responsible for* ***Process to Process Delivery****. Provides* ***QOS*** *through* ***Connection Oriented*** *and* ***Connectionless*** *transmission of IP datagrams in Transport layer packets. Uses Protocols Like TCP,UDP, SPX. Does* ***Port Addressing, Segementation and reassembly, Connection control Flow Control and error Control****.* |
| **Network Layer**<br>**Layer 3** | • *Responsible for End to End Transmission of* ***datagrams*** *across an Internetwork including Fragmenting , LOgical Addressing and Routing.Uses Protocols Like IP, IPX, NetBEUI.* ***Router*** *Operate at this Layer. Messaging unit is* ***Datagram*** *which includes IP addresses, identifying computers on Internetwork.* |
| **Datalink Layer**<br>**Layer 2** | • *Responsible for* ***packet*** *transmission betwween two systems on LAN. Does framing, Flow Control, error Control, Access Control and Physical Addressing. Messaging Unit is* ***Frame*** *and addressing through* ***Hardware Addresses (NIC Addresses).*** *Protocols Like Ethernet, Token Ring, etc. are used.* ***Bridges*** *and* ***Switches*** *Operate at this Layer.* |
| **Physical Layer**<br>**Layer 1** | • *Responsible for Transmission and reception of bits of data on /from the Medium, Signalling, Method and Cabeling, Representation of Bits, data Rate and Synchronization.* |

***Figure 2:*** *OSI Model*

## Filtering Techniques

Web Filtering techniques *[4, 5, 6, 7]* vary on the basis of their workings and the data they work upon. Figure 3 shows four possible filtering techniques namely rating based, blacklisting, keyword matching and dynamic that work upon different information associated with the web content. All of these filtering techniques can be used at the application layer of the OSI model but keyword matching and dynamic filtering can effectively be used only at application layer.

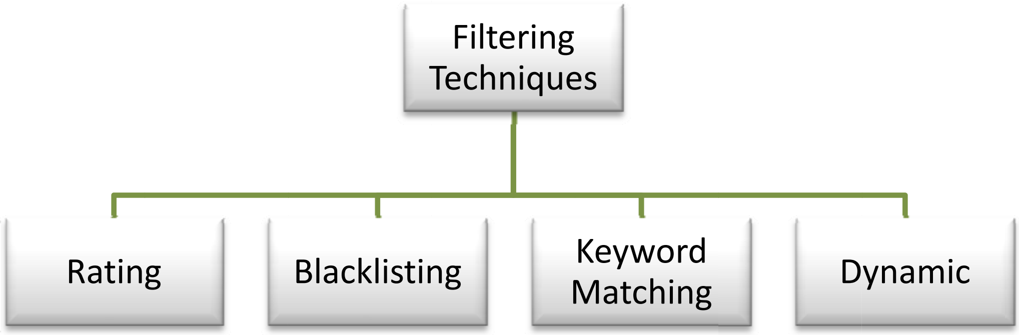

***Figure 3:*** *Filtering Techniques*

1. **Rating*:*** World Wide Web Consortium (W3C) has introduced a labelling system named Platform for Internet Content Selection (PICS) that defines a platform for creation of content labelling system. It enables the authors of the Web pages to include labels also called metadata that describes the content of the page. On the basis of this metadata third party rating authorities like Internet Content Rating Authority (ICRA) rates the website on the basis of presence or absence of certain elements in it. The ratings include ratings for Nudity, Sexual Content, Weapon Use, Drug Use, Violence, etc. A file is then generated containing ratings and the label that is linked to the domain of the Website. Web browsers like Internet Explorer, Safari, and Netscape include a Content Advisory mechanism that helps the users to regulate the content they want to block.

   This rating system is not regulated as some Web authors in order to evade the possibility of their Web content being blocked do not include metadata or include incorporate metadata in their Web content. Thus Content Advisors do not provide a foolproof solution and should be included as an additional line of defence against pornography.

2. **Blacklisting*:*** This technique uses a URL categorization database where URLs have been mapped to different categories according to their content. The Web filter policy

decides which categories to pass and which to block. The URLs belonging to the categories to be blocked constitutes the blacklist. The filter compares the requested URL against the blacklist and allows or denies this request accordingly. It is also possible to blacklist on the basis of IP address and Domain name besides URL Blocking at IP address level permits blocking of all domains hosted on the corresponding Web Server. Blocking at Domain name level blocks the entire domain.

The advantages of this method are speed and efficiency because the filter based on the blacklist has not to read the page before blocking or allowing.

Its disadvantages are the difficulties faced to create, and update the URL database as it is labour-intensive and requires human reviewers. Human reviewers nowadays have been replaced by automated filtering where a spider program automatically does categorization.

3. **Keyword *Matching:*** This type of filtering works by inspecting the web traffic for certain offensive words like ‘teen’, ‘sex’, ‘breast’ etc. and phrases, comparing them with its set of words and phrases to determine whether to allow or deny its access. Keyword matching filters is purely text-based methods. Keyword filtering is fast but over-blocking errors may be produced by this type of filter if the words labelled as offensive appear in legitimate web pages like sexton, breast cancer, etc. More precise content analysis methods can be used to reduce over-blocking but at the same time processing time will increase. Further, the efficiency of this filter for filtering pornography content is less because pornographic material often includes hefty data in pictorial and video formats.

4. **Dynamic *Filtering:*** These filters use various statistical machine learning methods like Baysian, k-Nearest Neghibour, etc. to understand the semantic content of the information to be filtered. They use multiple features; features from text (words like ‘sex’, ‘teen’, ‘gambling’, etc.), images (photographs in nudity), and possibly video clips. For filtering images for pornography colour, shapes and skin are investigated by algorithms like skin model, skin detection and regions of interest. Dynamic filters can be trained and continue to learn more with use. Several dynamic filters with reasonable efficiency to block pornography are available as commercial products.

Dynamic filters can also be used to construct and maintain blacklist categorization database.

Dynamic filtering offering advantage of automated filtering and learning capabilities can be designed to have higher efficiency but only at the cost of speed of operation making it unsuitable to be used at places like ISP and Organizational gateways.

## Comparison of Filters Installed at National Level in various Countries

Table 1 show below shows a comparison between Web Filters that are in place in Canada, United Kingdom, China and proposed filter of Australia.

| ***Australia*** | ***Canada*** | ***United Kingdom*** | ***China*** |
|---|---|---|---|
| ***Legislating Mandatory Filtering at ISP Level*** | | | |
| Yes | No | No | Yes<br>Around 20 pieces of legislation affects filtering |
| ***Voluntary/Industry Filtering at ISP Level*** | | | |
| Perhaps | Yes<br>Informal Government Pressure | Yes<br>Informal Government Pressure | Yes<br>Corporate Self-censorship is Prevalent |
| ***Opt-Out Provision*** | | | |
| No (Tier 1)<br>Yes (Tier 2) | No | No | No |
| ***Blacklist Filtering of Blocked URLs*** | | | |
| Yes | Yes | Yes | Yes |
| ***Purpose of Blacklist*** | | | |
| Unspecified | Blocking inadequate access to child pornographic material with HTTP protocol | Blocking inadequate access to child pornographic material with HTTP protocol | Blocking various types of illegal content |
| ***Type of Material Blacked*** | | | |
| Child Pornography and other illegal content | Child Pornography | Child Pornography | Political Content, Graphic Violence, Unapproved news, Child Pornography and other illegal content |
| ***Blacklist maintained by*** | | | |
| ACMA<br>Australian Communications and Media Authority | Cybertip.ca | Internet Watch Foundation | Ministry of Industry and information; Centre Propaganda Department; Ministry of Posts and Telecommunications |
| ***IP Address Blocking*** | | | |
| No | No | No | Yes |
| ***Deep Packet Inspection*** | | | |
| No | Yes | Yes | Yes |
| ***Purpose of Deep packet Inspection*** | | | |
| NA | Traffic Shaping | Traffic Shaping | Traffic Shaping, Dataveillance and Surveillance |
| ***Other Heuristic Methods*** | | | |
| Yes | Yes | Yes | Yes |

| Australia | Canada | United Kingdom | China |
|---|---|---|---|
| ***P2P*** | | | |
| No | Perhaps<br>Content infringement (in negotiation with music industry) | Perhaps Content infringement (in negotiation with music industry) | Yes |
| ***Instant Messaging*** | | | |
| No | No | No | Yes |
| ***Scope Creep*** | | | |
| Inevitable | Yes<br>Suicide sites, pro-terrorism sites, hate sites | Yes<br>Suicide sites, graphic terrorist beheading, pro-terrorism sites, hate sites | Yes<br>Legislation written with standard vague and ambiguous clauses such as the ‘state security’ provision |
| ***Offence to Circumvent Filters*** | | | |
| Yes<br>Not an offence to use circumvention devices such as proxy for other purposes | No | No | Yes<br>Not an offence to use circumvention devices such as proxy for other purposes |
| ***Legislative Safeguards*** | | | |
| No<br>No Bill of Rights, Constitutionally implied freedom of political communication very limited in this content and of little use as a safeguard | Limited<br>Charter of human Rights does not bind corporations such as ISPs (No legislation compelling ISPs) | Limited<br>Europe Convention on human Rights; relevant case law from European Court of Human Rights | No<br>The human rights instruments are of little practical significance (eg. Freedom of Expression is not an individual right) |
| ***Market Safeguard*** | | | |
| No<br>Compulsory for ISPs | Potentially<br>Voluntary initiative subject to strong informal government pressure | Potentially<br>Voluntary initiative subject to strong informal government pressure | None |
| ***Technical Safeguard*** | | | |
| No | Potentially<br>Depends where the filtering routers are placed (e.g. router located on the backbone would affect all ISPs) | Potentially<br>Depends where the filtering routers are placed (e.g. router located on the backbone would affect all ISPs) | Potentially<br>Geographic region of access and bandwidth capability affect ability to access material |

***Table 1****: Comparison between Web Filters that are in place in Canada, United Kingdom, China and proposed filter of Australia [8]*

It is apparent from the above comparison that no uniform criteria for filtering have been adopted by the compared countries apart from child pornography, URL Blacklisting, Instant Messaging, and Heuristic Methods. All other parameters for filtering vary from country to country.

## Effectiveness and Limitations

Filters vary widely in their performance, and there is a trade-off between failing to block unauthorized content called “under-blocking” and erroneously blocking authorized content called “over-blocking”. Filters that block a large percentage of unauthorized content also block a sizable percentage of authorized content in error. Web filters can make two types of errors namely false positive also called over blocking and false negative also called under blocking. Over blocking blocks permissible websites, raising issues about freedom of speech and legal issues clamming damage. Under blocking allows inappropriate websites to pass through the filter reducing its efficiency.

Several research works have reported that accuracy tests against filters do not provide a conclusive ranking about its efficiency. This is due to the fact that a filter may be highly accurate but it may be inefficient if only a few users are able to bypass it. Further, information on the Internet changes in a rapid and continuous manner forcing the filters to update at the same rate. A highly accurate filter may thus prove to be inefficient if it does not update itself with this change.

An ideal filter that neither produces false positive not false negative errors does not exist and thus a balance between the two filtering errors is highly desired. It has been found that filters are not efficient against those who manually exchange pornographic material. But filters reduce the availability of prohibited content and thus serve at least its modest objective of protecting innocent users against abuse and exposure to sensitive material.

## Conclusion

The study of web filtering reveals that filtering is possible at various places using a variety of filtering technologies which may operate at either network layer, transport layer or application layer of the OSI model. Depending upon the required customization of the filtering criteria, position of the filtering system is determined. Positions close to the main backbone leave no or very less filtering customization option for the ISP or the user. No specific filtering technique is having cent percent accuracy. The performance of a good filter may deteriorate unless it is constantly upgraded and maintained. The country level filtering mechanism does not adopt any universal criteria and instead filtering criteria is decided by its respective governments.

## Biographies

**M. Tariq Banday** was born in 1969. He did his M. Sc. and M. Phil. Degrees from the Department of Electronics, University of Kashmir, Srinagar, India in 1996 and 2008 respectively. He did advanced diploma course in computers and qualified UGC NET examination in 1997 and 1998. At present he is working as Assistant Professor in the Department of Electronics & Instrumentation Technology, University of Kashmir, Srinagar, India. He has to his credit several research publications in reputed journals and conference proceedings. He is a member of Computer Society of India, International Association of Engineers and ACM. His current research interests include Network Security, Internet Protocols and Network Architecture.

**Nisar A. Shah** was born in 1953. He did his M. Sc. and Ph. D. Degrees from the department of Physics, University of Kashmir, Srinagar, India in 1976 and 1981 respectively. At present he is working as Professor in the Department of Electronics & Instrumentation Technology, University of Kashmir. He has to his credit about 150 research publications which have been published in national and international journals of repute. He has supervised several research scholars in M. Phil. and Ph. D. programs. His current research interests include Digital Signal Processing and Network Security.

## References

[1]. Jose Maria Gomez Hidalgo, Enrique Puertas Sanz, Francisco Carrero Garcia, Manuel De Buenaga Rodriguez, (2009 ), “Chapter 7 Web Content Filtering”, In: Marvin V. Zelkowitz, Editor(s), Advances in Computers, Elsevier, Vol. 76, “Social Networking and The Web”, pp. 257-306, ISSN 0065-2458, ISBN 9780123748119, DOI: 10.1016/S0065-2458(09)01007-9.

[2]. W.Ph. Stol, H.K.W. Kaspersen, J. Kerstens, E.R. Leukfeldt, and A.R. Lodder, (2009), “Governmental filtering of websites: The Dutch case”, Computer law & security review, vol. 25, pp. 251–262.

[3]. Deibert R. J., Palfrey J. G., Rohozinski R., Zittrain J. (2008), “Access Denied; the Practice and Policy of Global Internet Filtering”. Cambridge, Mass: The Mitt Press; 2008.

[4]. Michael Chau and Hsinchun Chen, (2008), “A machine learning approach to web page filtering using content and structure analysis, Decision Support Systems”, vol. 44 pp. 482–494.

[5]. K. V. Chandrinos, Ion Androutsopoulos, G. Paliouras and C. D. Spyropoulos, (2000), “Automatic Web Rating: Filtering Obscene Content on the Web”, Lecture Notes in Computer Science, Volume 1923/2000.

[6]. Anirudh Ramachandran, Nick Feamster and Santosh Vempala, (2007), “Filtering spam with behavioural blacklisting”, proceedings of the 14th ACM conference on Computer and communications security, Pages: 342 – 351.

[7]. Patrick Reynolds and Amin Vahdat, (2003), “Efficient peer-to-peer keyword searching”, Proceedings of the ACM/IFIP/USENIX 2003 International Conference on Middleware, Pages: 21-40.

[8]. Alana Maurushat and Renee Watt, (2009), “Clean Feed: Australia’s Internet Filtering Proposal”, University of New South Wales, Faculty of Law Research Series, paper 7, 2009.

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

*Office*:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org