Deep Packet Inspection and Its Social Implications

Melih Kirlidog(*), Özgur Uçkan(**), Işık Barış Fidaner(***)

(*) Marmara University, Turkey / North-West University, South Africa
(**) Bilgi University, Turkey
(***) Bosphorus University, Turkey

Abstract

Technology can either be used for common good or for harming others. The latter, in some cases, involves using a more advanced type of technology for abusing the usage of a mainstream technology. Deep packet inspection (DPI) is a relatively new Internet technology that allows recognizing the applications and protocols among the data flowing through the servers of an Internet service provider (ISP). DPI can be used either for data traffic control and surveillance. The former is mainly used by the ISPs and the latter is by the governments. Both of them are regarded as threats for individual privacy and communication rights.

Keywords

Deep Packet Inspection, DPI, surveillance, profiling

I. INTRODUCTION

In general, the Internet has been merely a “dumb” communication medium since it was incepted four decades ago. This means that although it was prone to be eavesdropping like all other networks, it did not have any restrictions in content. In other words, it did not discriminate for or against any of its contents. Called *net neutrality* [1], [2], this tenet of the Internet was in conformity with its non-centralized and distributed growth path. The 90’s witnessed the introduction of the World Wide Web which accelerated the commercialization of the Internet. In the succeeding decade the Internet became a major political arena where some of its contents were created by its individual users and some others by political and social groups.

The Internet has been one of the fastest diffused technologies in human history. This is particularly true for the period after the introduction of the WWW. This fast diffusion transformed the Internet from merely a communication tool into a medium that supports a wide range of human activities spanning from entertainment to commercial activities. Communication, though, has been at the forefront of Internet usage. Like other traditional communication media such as telephone and surface mail, Internet communication is subject to abuse by governments or some other adversaries. Abuse of communication can take the form of opening private letters, wire tapping a telephone communication or eavesdropping to an e-mail that contains

some private message. There can be a wide range of motivations for performing such actions some of which could be legitimate and in accordance with law. However, many other cases involve blatant abuse of power by governments and other groups. Privacy advocates in many developing and industrialized countries struggle to expose and prevent such attempts, but such efforts are usually inadequate.

Deep packet inspection (DPI) is a technique in the Internet environment used to monitor or block the communication. This article will elaborate the DPI and its current implementations as well as the controversies it created in several countries including Turkey where there is an intense debate about Internet surveillance and privacy issues.

I.i. DPI and its implementation

The packets that form the data flow in the Internet have mainly two parts, namely the addresses of the source and destination nodes and the payload that makes up the content. The destination address of each packet is read by the routers and the packet is directed towards this address. Violating the “dumbness” and “neutrality” of the Internet, DPI software and hardware examine not only the destination address, but also the payload and the address of the sender. Then this information is compared with a set of signatures and protocols in order to identify the nature of the flowing data in the Internet Service Provider (ISP) hardware.

The data flow in the Internet environment is analogous to the letters processed in the post office. Normally, the letters are not opened in the post office and they are directed to the physical addresses written on the envelopes. The opposite is a clear privacy violation of the sender and receiver. The DPI is essentially the same.

As witnessed by the events in the Arab world in 2011, the Internet is an unprecedented facilitator for the social and political organizations of the ordinary people. It can also be functional for promoting hate speech and violence. Many governments have long been aware of this power and they are prone to implement control mechanisms on the Internet. DPI is the most prominent of these mechanisms which baffle techniques like proxy server usage. Many commercial organizations also profile Internet users with the aim of target marketing. To this end, they collect information about demographics, income, interests and habits of Internet users. For example, Facebook categorizes users with information in their Facebook pages. Categories like certain age groups, parents or locals in a country see relevant ads in their Facebook pages. Amazon also profiles its users based on the pages they visit on its website [3]. Although such profiling leads to very effective marketing, many regard it as a blatant violation of individual privacy. However, such profiling techniques are specific to individual web sites and not applicable outside of their user community. DPI offers a much broader surveillance mechanism for inspecting all of the activities of an Internet user. Such attempts led to severe reception from Internet users and organizations like European Union [4], [5].

There are mainly three types of DPI implementations. The first type is implemented by the advertisement industry. In this implementation the system assigns unique IDs to the users and monitors their activities on the web. As a result, the users are

profiled and targeted advertisements are applied on their screens. For example, if a user continuously visits the web sites related to babies, it is assumed that s/he has a baby or will have one in near future. The next step is to target that user with the advertisements of baby products. The second type of DPI implementation involves slowing down or blocking of the Internet lines for specific users according to their usage. For example, some applications like film downloading requires high bandwidth and the Internet Service Providers may choose to block or slow down such users. This, of course, is a clear violation of net neutrality. And lastly, the surveillance of the Internet by the governments is the third usage area of the DPI.

II. DPI AS A TECHNOLOGY

The DPI has its roots in the earlier intrusion detection systems (IDS). Unlike the host-based IDS which monitors the activities such as system logs and file modifications through a software agent in a host, network-based IDS monitors multiple hosts and the data traffic among them. A common way for the network-based IDS for detecting and sometimes blocking malicious activities is to compare the flowing traffic with the known signatures of the malicious attacks. Usually pattern matching techniques are used in this process [6]. This technical capability to detect and block malicious activity later paved the way for the development of DPI where not only malicious activities but all network traffic is monitored and classified according to the known signatures of the common applications and protocols such as VoIP and HTTP.

Packet inspection can be “deep” or “shallow.” Shallow packet inspection, which is sometimes called standard packet inspection, aims to extract only the IP addresses of the source and destination as well as other low-level connection states. This information exists in the packet header and does not give much hint about the application in transit which is typically held in the payload [7]. The requirement for application awareness can only be satisfied by analyzing the entire packet. This is a complex process that involves reassembling the packets to determine the source and destination of the flow as well as the application itself. The complexity is aggravated by the immense size of the data flowing through the ISP hardware that might have hundreds of thousands of users connected at a time. Hence, DPI requires extensive computing power which is directly proportional with the speed of the network. In the 7-Layer OSI model shallow packet inspection is mainly based on layer 2-3 and sometimes up to layer 4. DPI, on the other hand, operates in all layers from 2 to 7.

Some methods for network traffic analysis in the Internet have been proposed. One of them is the examination of the packet header for the TCP and TDP port number and mapping it to the commonly used ports. For example, port 80 is usually used for HTTP and port 53 is for DNS. However, determining the applications based on such rules is getting increasingly unreliable due to several facts such as the usage of obfuscation techniques including dynamic port numbers and port hopping in some applications. A recent study found that only 30%-70% of the Internet traffic can be identified with port-based approach [8]. Another method is to implement machine learning techniques for traffic analysis [9]. Port-based and machine learning techniques examine only the header of the packets and this has little to do with privacy violation. A thorough semantic traffic analysis requires the actual contents of the packet along with the header information. The DPI can provide such an analysis but it is prone to the privacy concerns.

Although it is difficult to bypass surveillance through DPI, a potentially effective method is encryption. Sending and receiving messages encrypted through commonly available systems like PGP or secure VPN can be implemented for privacy purposes. However, this has some drawbacks such as requirement for some basic technical knowledge and drawing the attention of the authorities. Additionally, it has little use against purposes like personal profiling by web site visits.

III. DPI AND LEGAL CONCERNS

Intercepting, modifying, examining, blocking, and copying the data communications with DPI has to deal with huge amounts of real-time data on both the Internet and 3G mobile networks. There are also some benefits of DPI with respect to several network management issues such as network optimization, data security, protection against network attacks.

On the other hand, it is also obvious that all such initiatives related with data communications make DPI a suitable tool for violating the rights and freedom of communication. For this reason, DPI has been a major focus of investigation during the last few years by the human rights advocates who deal with privacy, Internet censorship, net neutrality, freedom of expression and communication.

Regarding the use of DPI as a tool for violating the rights and freedom of communication, two principal actors are involved: corporations and governments. However, violations perpetrated by these two players are quite different in nature. Legal problems due to violations committed by corporations are usually limited to privacy issues. The fact that DPI is capable to examine massive data communications in real time and profile the habits of the Internet users and the content of their communication content makes it especially attractive for a series of commercial applications such as targeted advertising and content based pricing. But such capabilities can easily be extended to other extraordinary usages: monitoring of communications of company employees, customers and business partners, mass personal surveillance, industrial espionage, high volume copyright theft, trademark infringement, etc. Furthermore, DPI can be deployed to prioritize data communication for unfair competition. And this can further encourage noncompetitive tendencies in network operations by providing unfair advantages for a certain service or service provider. For example, some telecommunication companies use DPI to prioritize their own services (e.g. IPTV) by making life more difficult for competitor service providers.

Governments in many countries are usually curious about their citizens' communications which reflect their private lives. Even so-called democratic countries do not respect and consequently breach their own regulations about individual privacy and the right of communication. It is widely known that, based on the HADOPI legislation in France which is also called as the “three-strike-out” and OPPSI laws that legitimize mass monitoring. Behind the excuse of the fight with terrorism, DPI based systems are about to be used to monitor the whole population [35], [36]. Also in the USA the use of DPI by the government for unlawful interception is quite common [37] and institutions such as Free Press call the voters to be aware of this situation [38].

Another example is from the UK with a company named Phorm. Phorm has started its activities in the US with the name 121Media. It is specialized in the DPI implementation of targeted advertisements. Thanks to the activities of the US citizens and NGOs that are sensitive about privacy issues, the company had to cease its operations in the US. The next step for Phorm was to move to the UK where its system ("Webwise") was used as trial by some large ISPs like BT, Virgin Media and TalkTalk. During these trials the users were not informed and a large campaign was started against Phorm when it was disclosed that it was monitoring the activities of Internet users. The EU was also involved and threatened the UK Government by going to court if it does not stop Phorm's activities in the country. After thousands of signatures and a court case against, the company had to cease its operations in the UK. It is worth noting that the British Government that does not seem to care much about its citizens' privacy and communication rights openly supported Phorm during this process. It is possible that the Government had hoped to develop Phorm's technology further for surveillance issues.

Richard Clayton, who comments from a legal point of view, explains the Phorm architecture as follows: "The basic concept behind the Phorm architecture is that they wish to take a copy of the traffic that passes between an end-user and a website. This enables their systems to inspect what requests were made to the website and to determine what content came back from that website. An understanding of the types of websites visited is used to target adverts at particular users" [10]. The usage of this system by the British ISPs has triggered much criticism among netizens and privacy advocates. The Foundation for Information Policy Research has published two separate legal analyses and indicated that such usage violated the British Law in the following areas: interception of communications, an offence contrary to Section 1 of the Regulation of Investigatory Powers Act 2000; fraud, an offence contrary to Section 1 of the Fraud Act 2006; unlawful processing of sensitive personal data, contrary to the Data Protection Act 1998; risks of committing civil wrongs actionable at the suit of website owners such as the Bank of England; use of private communication traffic will infringe the Copyright, Designs and Patents Act 1988 [11], [12]. During a debate held at the British Parliament where Phorm was discussed at length, Tim Berners-Lee reports the following: "... a healthy web for society places requirements also on the Internet layer. In 2008, this was threatened in the UK by the company Phorm proposing to use data from deep packet inspection (DPI). The system would use special apparatus at the ISP to monitor traffic, peek inside the IP packet's payload, and determine every URL looked in a household's browsing on the web. This profile would be used to provide targeted advertising. (...) The Internet in general has and deserves the same protection as paper mail and telephone. In fact you could argue that it needs it more, as it carries more or our lives and is more revealing than our phone calls or our mail. The access by an ISP of information within an Internet packet, other than that information used for routing, is equivalent to wiretapping a phone or opening sealed postal mail. The information could be deliberately abused by an inside worker, or could be acquired by an attack on the system's machines. The power of this information is so great that the commercial incentive for companies or individuals misuse it will be huge, so it is essential to have absolute clarity that it is illegal. To put this in perspective, it is like the company having a video camera inside your house, except that it gives them actually much more information about you. The act of reading, like the act of writing, is a pure,

fundamental, human act. It must be available without interference or spying [13]. As can be seen in this example, use of DPI, especially by ISPs and telecoms, poses great risks in terms of violation of both privacy and net neutrality and therefore, should be checked, by legislation. Federal Communications Commission in the US also maintained, in its report on the ISP Comcast's violation of privacy, that a strict legal standard should be introduced to the use of DPI [14].

The misuse of DPI by the governments can be more abusive and harmful than corporations. Overreaching and unlawful exploitations by governments are, by their very extent, more devastating in terms of violating individual rights and freedoms. These are, beyond the right of privacy, also communication rights such as freedom of communication, freedom of expression and freedom of information, which are, usually defined as the third generation of human rights.

As DPI technology offers, beyond listening, monitoring and tracking of the communication content, that is, keeping records of the Internet users, also several means for manipulating, changing and blocking such content, it thus provides very convenient mechanisms for filtering and censuring the Internet. Equipped with such capabilities, DPI poses a threat not only against privacy rights, but also the right of communication.

III.i DPI and surveillance in the developing world

The most spectacular example showing the usage of DPI for violating the right of communication was the initiative of the Egyptian Government, a first ever in the short history of the Internet on 28 January 2011: starting at 22.28 (UTC) on 27 January 2011, the Egyptian Government shut down all the Internet, mobile network and land-based communication, thus preventing data and voice communications carried over these networks. That is, everything else except the satellite communication, something they could not control at all. Until the Internet resumed its normal "censored" status on 2 February 2011, the whole country became a big black hole in the global network. This was a historical first [15]. It was introduced mainly because of two reasons: first, to block communication among protesters the number of which was expected to reach millions; second, to isolate Egypt from the rest of the world and thus enjoy the liberty to crash the uprising brutally. Meanwhile, it was understood that the Egyptian Government collaborated with the American company "Narus Insight", a Boeing subsidiary that also has contacts with Israel and Pentagon, for both the shut down of the Internet and monitoring the Internet traffic of the opponents. It became clear that the company sold DPI-based tracking, censoring and "kill switch" systems to the Egyptian telecom enterprise [16], [17]. Once this news became public, Free Press started an initiative for the monitoring of DPI sales and usage [18], [19]. The fact that the DPI technology, to which governments have been trying to give an dubious legitimacy with the branding of "lawful interception," has caused severe human rights violations when used by dictators within the framework of their local law systems, stimulated considerably public sensitivity. Currently, several examples are experienced. For example, it was revealed that just a few years before the Tunisian Revolution which culminated with the escape of Ben Ali on 14 January 2011 and thus started the "Arab Spring", the public institutions of Agence Tunisienne d'Internet (ATI) and Agence Tunisienne de Communication Exterieure (ATCE) created a DPI-based monitoring system to censure the Internet, to excessively monitor it and to keep

records of the cyber dissidents with the helping hand of a French company [20], [21], [22], [23], [24], [25]. The identity of this company is still on investigation. Indeed, the existence of this system was common knowledge even before the revolution. Similarly, it became public that Nokia – Siemens jointly sold DPI-based systems to Iran [26], [27], [28]. Cisco and China's relationship in the "Golden Shield Project" of the "Great Firewall" is still fiercely debated. Some Chinese dissidents who claim that they were subject to some damages because of the DPI-based systems provided by Cisco to the Chinese Government filed suit [29]. The last exemplary case is the situation in Syria. It is claimed that BlueCoat, a USA firm, has sold DPI-based tracking and censoring systems to the Assad regime [30], [31], [32]. It is further claimed that Assad trained his agents in Tunisia during the Ben Ali government. Indeed, methods which prevent Facebook connections to secure servers (https) and instead redirect to regular (http) servers where users can be monitored, look quite similar to those used in Tunisia [33].

Such examples can be multiplied. Civil rights and freedoms activists consider such relationships as selling digital mass destruction weapons to authoritarian regimes. During a broadcast of the Office of the Privacy Commissioner of Canada, it has been stated that a series of countries which have a very bad score of human rights and where the barest principles of net neutrality are not observed, have been using DPI based monitoring and censuring systems: China, Burma, Vietnam, Tunisia, Saudi Arabia, Yemen, Ethiopia, UAE, Syria, Pakistan, Iran, Uzbekistan, Kyrgyzstan and Belarus [34].

Since 11 September 2001, governments are in a kind of race to introduce regulations that tip the balance between security and freedoms and thus erode universal human rights. Such regulations focus on the control of the Internet, the very medium that represents the new horizon of civil rights and freedoms. Therefore, in a setting where we are expected to trade our freedom for security concerns, abusive technologies such as the use of DPI emerge, under the pretension of the "lawful interception" brand, as a big threat not only in authoritarian countries but also in those who are willing to sacrifice their democracies.

This can be countered by claiming that DPI is a technology which has some "benefits", too. But its "disadvantages" are clearly obvious. Citizens do have the right to expect from their governments to act transparently, responsibly and be accountable on such an issue that simply amounts to a direct violation of our constitutional privacy and communication rights.

III.ii. Turkey: Possible uses of DPI

Like most countries in the world, there are problems for the rights of communication with respect to third generation of human rights in Turkey [39], [40]. As this negative setting also includes the very right of access to information, it is not possible to obtain clear and healthy information on a good deal of issues related with civil rights and freedoms. For example, in spite of our requests based on the Freedom of Information Act and questioning the possible uses of DPI by the Telecommunications Communication Presidency (TIB), the legal authority responsible for such matters, we were not able to receive a meaningful response. Therefore, in this section, we will be content by making some inferences based on the news circulating in the media.

It is reported that Turkey has been implementing the so called “National Network Tracking Center” (UNIM) project via the Information Technologies and Communications Authority (BTK) and its Telecommunications Communication Presidency department, since a few years. It is claimed that DPI methods are used in this project [41], [42], [43], [44], [45]. The timing of the first discussions of this project coincides with the massive disinformation efforts that supposedly targeted child pornography and were carried out prior to the introduction of the “Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publication” Act Nr. 5651 to censure the Internet. As it is usually known, concepts such as child pornography and war on terrorism are widely used to justify the said abusive regulations and implementations [46].

Mustafa Akgul, President of Internet Technologies Association (INETD), argued that BTK installed some “black boxes” at ISP level to eavesdrop VOIP communications and INETD sued BTK for privacy violation [52]. Nate Anderson makes a reference on this kind of “black boxes” as CALEA-compliant DPI system(s)”: “Much DPI gear is also CALEA-compliant. The boxes generally contain an “aux” port that can spit out a real-time copy of any required information: all traffic from a specific IP address, e-mail, Internet phone calls, URLs. The rules are simply programmed into the box’s GUI and bam!—instant surveillance” [53].

Meanwhile, it is also known that DPI is widely used by several corporations, including mobile telephone operators [54], [55]. The implementation of the UNIM project is not transparent. But there are rumors that BTK works with a company called C2Tech [56] which sells DPI solutions [57]. It is also reported that the Prime Minister ordered the establishment of an Internet tracking unit within the Ministry of Transportation and the BTK [58]. As usual, it is argued that the unit will mainly be responsible to monitor the Internet communication of the “terrorists.” However, there is no guarantee that ordinary citizens will not be eavesdropped by the new hardware that is to be acquired. In conclusion, we can say that there is strong evidence regarding the use of DPI by both the corporations and the government in such a way as to violate the basic rights and freedoms. Public authorities do not act in a transparent and accountable way regarding civil rights and freedoms. Instead, they tend to consider censorship and monitoring as basic methods for governing and such use of DPI is a serious threat for all citizens. A cautious monitoring of the international institutions sensitive to civil rights and freedoms, including the European Union which Turkey is trying to join, and a more active role in inviting the authorities to act transparently, might provide some assistance to the problem.

Recently Phorm has announced that it has started operating in Turkey. The company is currently operating in Turkey, Brazil and Romania all of which are regarded as developing countries. Internet users in industrialized countries are sensitive to privacy issues and they tend to claim their digital rights. It seems that Phorm has acknowledged this after some bitter experiences and has decided to try its luck in developing countries. It is yet to be seen whether its attempt will be successful or not.

It must be noted that, as opposed to the companies like Phorm that are specialized in advertisement industry, DPI companies that are specialized in government

surveillance usually do not have the problem of strong opposition from civil society. There are numerous such companies and they sell their products to developing and industrialized companies without much difficulty [37]. Concepts like “national defense” and “fight against terrorism” make their job much easier compared to DPI companies specialized in advertisements. This is due to the fact that the latter have little to offer to the Internet users other than violating their privacy.

IV. CONCLUSION

DPI is currently being used by many Governments and commercial organizations all around the world and it is the major source of privacy concerns in the Internet environment. It will increasingly be subject to debate among the parties and its abuse by Governments and commercial organizations can only be prevented by the awareness of ordinary citizens.

The answering of the questions posed by Christopher Parsons are critical for the future of both the Internet which started a new era of social, cultural and economic dimensions, and civil rights and freedoms: “We are amid a standardization revolution, a mass translation of discordant analogue signal types into interoperable digital transmission standards. Speech, writing, and video now traverse the globe at near light speed via spider-like networks of fiber-optic cables, and all of this digitized consumer traffic to and from the Internet passes through the ISPs gateways. ISPs, as communicative bottlenecks, are ideally situated to monitor, mine, and modify data using the deep packet inspection (DPI) appliances situated within their networks. Around the globe, communications are mediated by DPI equipment in service of the respective interests of ISPs, advertisers, governments, and copyright lobbies. DPI’s broad capacities—and the attention given to the technology by the abovementioned actors—have piqued the interest of researchers in various fields of the social sciences. Common questions are beginning to emerge, including: who is driving deep packet inspection? What is DPI’s role in network management? How (and why) have copyright lobbies, advertisers, and government taken an interest in monitoring data communications? What uses of the technology are considered legal, and in what cases are privacy interests endangered by the technology?”[59] This paper aimed to contribute to answering these crucial questions.

ACKNOWLEDGMENT

The authors would like to thank Mutlu Binark and Ali Riza Keles¸ from Alternative Informatics Association for their contribution to this article.

REFERENCES

[1] P. Ganley and B. Allgrove, “Net neutrality: A user’s guide,” *Computer Law & Security Report*, vol. 22, no. 6, pp. 454– 463, 2006.

[2] F.-Y. Ling, S. - L. Tang, M. Wu, Y.-X. Li, and H.-Y. Du, “Research on the net neutrality: The case of Comcast blocking,” in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, aug. 2010, pp. V5–488 –V5–491.

[3] L. Christiansen, “Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven,” *Business Horizons*, vol. In Press, Corrected Proof, pp. –, 2011.

[4] A. McStay, “Profiling Phorm: an autopoietic approach to the audience-as-commodity,” *Surveillance & Society*, vol. 8, no. 3, pp. 310 – 322, 2011.

[5] H. Kemmitt, M. Dizon, T. Gastrell, and S. Lewis, “EU update,” *Computer Law & Security Review*, vol. 27, no. 1, pp. 86 – 91, 2011.

[6] Z. Chen, Y. Zhang, Z. Chen, and A. Delis, “A digest and pattern matching-based intrusion detection engine”*The Computer Journal*, vol. 52, no. 6, pp. 699–723, 2009. [Online]. Available: http://comjnl.oxfordjournals.org/content/52/6/699.abstract

[7] K. Xu, J. Tan, L. Guo, and B. Fang, “Traffic-aware multiple regular expression matching algorithm for deep packet inspection,” *Journal of Networks*, vol. 6, no. 5, pp. 799 – 806, 2011.

[8] A. Madhukar and C. Williamson, “A longitudinal study of P2P traffic classification,” in *Proceedings of the 14th IEEE International Symposium on Modeling, Analysis, and Simulation*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 179–188.

[9] J. Erman, A. Mahanti, and M. Arlitt, “QRP05-4: Internet traffic identification using machine learning,” in *Global Telecommunications Conference, 2006. GLOBECOM ’06. IEEE*, 27 2006-Dec. 1 2006, pp. 1–6.

[10] R. Clayton, “The Phorm “webwise” system,” May 18, 2008. [Online]. Available: http://www.cl.cam.ac.uk/ rnc1/080518-phorm.pdf

[11] N. Bohm, “The Phorm “webwise” system - a legal analysis,” April 23, 2008. [Online]. Available: http://www.cl.cam.ac.uk/ rnc1/080518-phorm.pdf

[12] N. Bohm and J. Harrison, “Profiling web users – some intellectual property problems,” November 2008. [Online]. Available: http://www.fipr.org/0811SCLarticle.pdf

[13] T. Berners-Lee, “No snooping,” March 9, 2009. [Online]. Available: http://www.w3.org/DesignIssues/NoSnooping.html

[14] Federal Communications Commission, “Memorandum opinion and order,” August 1, 2008. [Online]. Available: http://hraunfoss.fcc.gov/edocs public /attachmatch/FCC-08-183A1.pdf

[15] J. Cowie, “Egypt leaves the Internet,” January 27, 2011. [Online]. Available: http://www.renesys.com/blog/2011/01/egypt-leavesthe-internet.shtml

[16] J. Ettinger, “Questions raised about US firm’s role in Egypt Internet crackdown,” January 28, 2011. [Online]. Available: http://www.freepress.net/press-release/2011/1/28/questionsraised-about-us-firms-role-egypt-internet-crackdown

[17] T. Karr, “One US corporation’s role in Egypt’s brutal crackdown,” January 28, 2011. [Online]. Available: http://www.huffingtonpost.com/timothy-karr/one-us-corporationsrole-b 815281.html

[18] Free Press, “Free Press is calling for Congress to investigate the use and sale of DPI technology by American companies. Add your name to our letter now.” February 2011. [Online]. Available: http://act2.freepress.net/sign/dpi/?rd=1&t=6&referring akid =2263.9178450.Z4wClC

[19] NoDPI. [Online]. Available: https://nodpi.org/

[20] S. Amamou, “Op´eration massive de phishing sur Gmail en Tunisie,” June 29, 2010. [Online]. Available: http://fr.readwriteweb.com/2010/06/29/nouveautes/oprationmassive-de-phising-sur-gmail-en-tunisie/

[21] F. Epelboin, “Le Deep Packet Inspection : pour mieux vous (a)servir,” January 12, 2010. [Online]. Available: http://fr.readwriteweb.com/2010/01/12/analyse/deep-packetinspection-censure-filtrage/

[22] tekiano.com, “Tunisie : L’ATCE a censur´e le Net, pas l’ATI !” January 31, 2011. [Online]. Available: http://www.tekiano.com/net/web-2-0/2-7-3132/tunisie-latce-a-censure-le-net-pas-lati-.html

[23] F. Epelboin, “Manipulation de masse : un oeil sur l’avenir de la communication politique dans les r´eseaux,” May 19, 2011. [Online]. Available: http://reflets.info/manipulation-de-masse-un-oeil-sur-lavenirde-la-communication-politique-dans-les-reseaux/

[24] Nawaat.org, “Tunisie : La toile emprisonn´ee,” August 19, 2010. [Online]. Available: http://nawaat.org/portail/2010/08/19/tunisie-la-toileemprisonnee/

[25] C. Parsons, “Technology and politics in Tunisia and Iran: Deep packet surveillance,” March 23, 2011. [Online]. Available: http://pactac.net/2011/03/technology-and-politics-in-tunisiaand-iran-deep-packet-surveillance/#more-780

[26] C. Rhoads and L. Chao, “Iran’s web spying aided by western technology,” June 23, 2009. [Online]. Available: http://online.wsj.com/article/SB124562668777335653.html#mod=rss whats news us

[27] K. Zetter, “WSJ: Nokia, Siemens help Iran spy on Internet users,” June 22, 2009. [Online]. Available: http://www.wired.com/threatlevel/2009/06/wsj-nokia-and-siemenshelp-iran-spy-on-internet-users/

[28] T. Karr, “Helping Iran target Iranians,” July 10, 2009. [Online]. Available: http://www.huffingtonpost.com/timothy-karr/helpingiran-target-irani b 229369.html

[29] R. Reitman, “Cisco and abuses of human rights in China: Part 1,” August 22, 2011. [Online]. Available: https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-humanrights-china-part-1

[30] kitetoa, “De l’´ethique dans les affaires (informatiques),” August 19, 2011. [Online]. Available: http://reflets.info/de-lethique-dans-lesaffaires-informatiques/

[31] bluetouff, “#OpSyria: Web censorship technologies in Syria revealed [EN],” August 12, 2011. [Online]. Available: http://reflets.info/opsyriaweb-censorship-technologies-in-syria-revealed-en/

[32] Streams of WikiLeaks, “Stop bluecoat.com now #OpSyria #Syria #emcom,” August 21, 2011. [Online]. Available: http://newsintercom.tumblr.com/post/9187075188

[33] The Register Forum, “Fake certificate attack targets Facebook users in Syria,” May 6, 2011. [Online]. Available: http://forums.theregister.co.uk/forum/1/2011/05/06/syria fake

certificate facebook attack/

[34] Office of the Privacy Commissioner Of Canada, “DPI: The future is out there,” 2011. [Online]. Available: http://dpi.priv.gc.ca/index.php/essays/dpi-the-future-is-out-there/

[35] bluetouff, “Deep Packet Inspection : le DPI qui civilise les Internets,” June 1, 2011. [Online]. Available: http://reflets.info/deeppacket-inspection-le-dpi-qui-civilise-les-Internets/

[36] ——, “Deep Packet Inspection : retour sur la rencontre avec le PDG de Qosmos,” February 26, 2011. [Online]. Available: http://reflets.info/deep-packet-inspection-qosmos-techtoctv/

[37] J. Bamford, *The Shadow Factory*. New York: First Anchor Books Edition, 2009.

[38] J. Silver, ““Deep Packet Inspection:” from Iran and China... to America.” [Online]. Available: http://www.savetheInternet.com/video/31272#

[39] Y. Akdeniz and K. Altıparmak, “Internet: Restricted access – A critical assessment of Internet content regulation and censorship in Turkey,” November 2008. [Online]. Available: http://www.cyberrights.org/reports/Internet restricted colour.pdf

[40] Y. Akdeniz, “Report of the OSCE representative on freedom of the media on Turkey and Internet censorship,” January 2010. [Online]. Available: http://www.osce.org/documents/rfm/2010/01/42294 en.pdf

[41] S. Güneç, and S. Kuvel, “Sanal suça büyük gözaltı; Internet Takip Merkezi geliyor,” December 15, 2006. [Online]. Available: http://www.zaman.com.tr/haber.do?haberno=472009

[42] M. Sakin, “Internet Takip Merkezi olsun; ama iletisim özgürlüğünü kısıtlamasın,” December 16, 2006. [Online]. Available: http://www.zaman.com.tr/haber.do?haberno=472686

[43] G. Ahi, “Çocuk pornosu bahane Internete sansür şahane,” December 29, 2006. [Online]. Available: http://www.hurriyet.com.tr/eyasam/5693403.asp?gid=54&srid=3099&oid=6&l=1

[44] U. Dolgun, “‘Büyük Birader’in ayak sesleri internet sayesinde daha da güçlü” December 28, 2006. [Online]. Available: http://www.radikal.com.tr/haber.php?haberno=208500

[45] Özgür Uçkan, “Internet sansüründen, mahremiyet ve iletişim özgürlüğü ihlaline,” August 24-30, 2009. [Online]. Available: http://ozguruckanzone.blogspot.com/2009/08/oyunun-kural-Internet-sansurunden.html

[46] ——, “Çocuk istismarından Internet istismarına Türkiye,” August 2009. [Online]. Available: http://www.ozguruckan.com/kategori/politika/22243/cocukistismarindan-Internet-istismarina-turkiye

[47] Y. Akdeniz, “OSCE Report on Freedom of Expression on the Internet: Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States, The report has been commissioned by the Office of the OSCE Representative on Freedom of the Media,” p. 26. [Online]. Available: http://www.osce.org/fom/80723

[48] Özgür Uçkan, “22 Ağustos: Türkiye Internetinin kara deliği,” July 2011. [Online]. Available: http://www.gennaration.com.tr/yazarlar/22-agustos-turkiye-internetinin-kara-deligi/

[49] Alternative Informatics Association, “Ongoing mandatory filtering imposed by the State: Misleading strategy about safe Internet use in Turkey,” August 6, 2011. [Online]. Available: http://yenimedya.wordpress.com/2011/08/07/1775/

[50] I. Öz, “Prof. Binark: Güvenli internet adıyla kamuoyu yanıltılıyor!” August 27, 2011. [Online]. Available: http://www.t24.com.tr/profbinark-guvenli-internet-adiyla-kamuoyu-yani/haber/165071.aspx

[51] K. Altıparmak and Y. Akdeniz, “Zorunlu değil ama sorunlu filtreleme,” August 15, 2011. [Online]. Available: http://privacy.cyberrights.org.tr/?p=1480

[52] Teknopolitika, “Mustafa Akgül’le ‘22 Ağustos sonrası ve Internette sansür’ üzerine söyleşi,” August 25, 2011. [Online]. Available: http://www.sendika.org/yazi.php?yazi no=39298

[53] N. Anderson, “Deep packet inspection meets ‘Net neutrality’, CALEA,” 2008. [Online]. Available:http://arstechnica.com/hardware/news/2007/07/Deep-packetinspection-meets-net-neutrality.ars/4

[54] T. Sırt, “Sanal müfettiş¸!” May 16, 2011. [Online]. Available: http://www.sabah.com.tr/Teknoloji/Blog/2011/05/16/sanal-mufettis

[55] BTM, “DPI deployments (74): Vodafone Turkey uses Optenet and Allot for web filtering,” June 25, 2011. [Online]. Available: http://broabandtrafficmanagement.blogspot.com/2011/06/dpideployments-74-vodafone-turkey-uses.html

[56] C2Tech, “C2Tech / Technologies / Deep Packet Inspection,” 2011. [Online]. Available: http://www.ctech.com.tr/technologies/deep-packetinspection

[57] Özgür Uçkan, “‘Deep Packet Inspection’ ve ‘Ulusal Network Izleme Merkezi’,” September 5-11, 2011.

[58], “Kandil Internetten de vurulacak,” August 19, 2011. [Online]. Available: http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1060531&Date=19.08.2011&CategoryID=77

[59] C. Parsons, “Literature review of deep packet inspection: Prepared for the new transparency project’s cyber-surveillance workshop,” p. 2, March 6 2011. [Online]. Available: http://www.christopher-parsons.com/blog/ wpcontent/uploads/2011/04/ Parsons-Deep packet inspection.pdf