

The Hidden Impacts of Anti-Spam Measures and their Contribution to the Digital Divide: An Exploratory Study¹

Christopher P. Lueg

School of Information Technology, Charles Darwin University, Darwin, Australia. E-mail: lueg@cdu.edu.au

Proliferation of unrestricted Internet access has brought the community unsolicited commercial email, better known as spam. Underestimated for quite some time, spam is now recognized as a problem costing the community billions of dollars per annum. One of the direct impacts of the spam flood is the widespread deployment of anti-spam measures, such as email filters and block lists. In this paper, we summarize scholarly and anecdotal evidence suggesting that apart from reducing the spam load, anti-spam measures are also undermining the email system in terms of reliability and usability. Furthermore, we discuss findings suggesting that anti-spam measures are also contributing to establishing a digital divide between those having a choice as to how they access email (both from a technical perspective and an educational point of view) and those who are not in this favorable position.

Introduction

Proliferation of unrestricted Internet access has brought the community unsolicited commercial email, commonly referred to as "spam". Underestimated for too long, spam has become a major problem costing the community billions of dollars per annum. As a consequence, anti-spam technologies have been deployed widely. The two main anti-spam technologies are filtering and blocking. Filtering technology is used to remove emails containing terms, such as "warez", "get rich quick" or "free porn", that have shown to be typical of spam messages. Block lists are used to prevent suspicious mail servers from delivering mail to one's own mail server.

Most studies in the context of spam focus on quantifying spam (e.g., Cranor and LaMacchia 1998; Aberdeen 2002; Ferris 2002), characteristics of spam (e.g., FTC 2003) and ways to fight spam (e.g., NOIE 2002). A notable exception is Fallows' (2003) study on the perception of spam and how it changes the way people use email. Findings of Fittkau and Maaß' (2004) online survey seem to support some of these impressions.

Personal experiences with anti-spam technology (genuine business email not delivered because it was suspected to be "spam") suggest this technology is not "neutral" in the sense that there are no side-effects. The possibility of such side-effects is mentioned in the literature (e.g., Geer 2004) but has not been explored yet. The purpose of this exploratory study is to describe in more detail secondary impacts of anti-spam measures as far as they can be deduced from the literature and other sources. The latter are important as there are very few relevant journal papers;

most sources are reports, newspaper articles, web sites maintained by anti-spam activists and by companies in the anti-spam business. Another important information source are statements in spam-related Internet discussion forums. The prevalence of "informal" sources results from both the speed at which the spam problem has emerged and the occupation of key players who are often employed as technical staff or system administrators. Accordingly, the research method is mainly descriptive/interpretive. Interpretations are also influenced by the author's participation in spam fighting and system administration activities since 1995.

The paper is structured as follows. First, we briefly review definitions of spam and some of the acknowledged impacts of spam. Next, we discuss the primary -intended-effects of anti-spam measures and how they are accomplished. Then, we present the first of the two main contributions of this paper: a broad discussion of secondary -unintended- effects of anti-spam measures and how these effects manifest. As the second major contribution, we look at secondary effects of anti-spam measures and argue that they contribute to the digital divide. The paper closes with a summary and a look at future research in the area.

Spam and Acknowledged Impacts of Spam

In this section, we provide some background information regarding the spam phenomenon: definitions of spam, difficulties involved in creating such definitions as well as some quantitative data about spam. We also look at some of the better known impacts of spam which are economical impacts and psychological effects.

Definitions of Spam

Baseley (1998) highlights that originally, the term "spam" referred to a specific kind of Usenet (NetNews) posting rather than email. In the meantime, however, using the term for a specific kind of unwanted email has become common practice.

Typically, the term "spam" is used as a colloquial and more convenient replacement for "unsolicited commercial email" (UCE). The origin of using the term "spam" for unwanted postings or email is unclear; the prevailing theory is that the term is derived from the song in Monty Python's famous spam-loving vikings sketch (Southwick and Falk 1998).

Mueller (2003) provides a spam definition covering both Usenet postings and email: "Spam is flooding the Internet with many copies of the same message, in an attempt to

¹ To appear in the Proceedings of the Annual Meeting of the American Society for Information Science and Technology (ASIS&T), Providence/Rhode Island, November 13-18, 2004.

force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender."

A report by the U.S. Federal Trade Commission's Division on Marketing Practices investigating false claims in spam (FTC 2003) supports the impression that a good part of spam messages is fraudulent, finding indicators of false claims in two-thirds of the messages investigated. The report does not provide a precise definition of what was regarded as spam; the report merely states unsolicited commercial email (UCE) is commonly known as spam.

In a report on the spam problem and how it can be countered, the Australian National Office for the Information Economy (NOIE 2002) defines spam as "unsolicited electronic messaging, regardless of its content" (p. 7). The report explicitly mentions that "arriving at an agreed definition of spam is a potentially contentious issue, as the direct marketing industry, ISPs, spammers, blacklists and privacy and consumer groups have their own interests and views." The report does not define what is understood as "unsolicited" either.

Similarly, the U.S. Center for Democracy and Technology states that "spam is used to refer to a single or multiple pieces of mail that are perceived by the recipients to be unsolicited and unwanted" (CDT n.d.) without defining what is meant by "unsolicited" or "unwanted".

Baseley (1998) discusses the rather important difference between "solicited email" and "unsolicited email". Lueg (2003) points out that in many situations the differences are fuzzy and at least to some extent in the eye of the observer. While most would agree that the infamous "Nigeria" scam classifies as spam deserving to be removed, opinions may be divided in the case of political messages or jokes. Based on a recent survey, Fallows (2003) provides empirically derived support for this view: "While Internet users generally agree that spam is 'unsolicited commercial email from a sender you don't know,' there is plenty of room for fuzziness around the edges. Messages with religious, political, or charity-fundraising content is spam to some, but not others. Users also have varying answers about how businesses should interpret their relationship with potential customers. There is not a clear consensus among users about the circumstances under which they are 'known' by a seller or 'have a relationship with' a firm." (p. ii).

Lueg (2003) illustrates that the problems around defining "solicitedness" in precise technical terms mean it is unlikely that there will ever be a precise definition of spam. Operationalizing such a definition, however, is a prerequisite for reliable filtering of spam messages. Fallows (2003) also points out that the problem of defining spam from a user's perspective is "an issue that is an absolute stopper for writing effective, enforceable legislation against spam."

Quantifying Spam

Cranor and LaMacchia (1998) describe one of the first attempts to quantify spam. Analyzing the mail intake at selected AT&T and Lucent mail sub-domains, Cranor and LaMacchia report that in April 1998 2.5% of all email would classify as spam. This figure was less than expected as AOL reported a 30% spam figure. They suggest AOL's spam intake may not be typical for businesses in general as AOL users might attract an unusually high number of spam messages. Cranor and LaMacchia also report, however, that between April 1998 and August 1998, the end of their study, the amount of spam sent to the AT&T and Lucent sub-domains under observation had doubled to 5% from 2.5%.

In a 2002 study, market researchers Aberdeen Group estimate the spam proportion in corporate networks to be around 25% of all emails and expected the proportion to reach 50% within 2003 (Aberdeen Group 2002). Anecdotal evidence (personal communication) suggests that some enterprises have reached the 50% threshold in mid 2003. Similar figures were mentioned by an enterprise systems consultant quoted in Fallows (2003): "For my most recent customer, spam accounts for more than 50% of all the email flowing into their systems." (p. 22). There is some evidence that the amount of spam is now close to 80% even in corporate networks.

In a press release published end of 2003, AOL (2003) states they blocked 500 billion -or a half-trillion- spam emails from getting to the inboxes of its members during the 2003 calendar year. In average they removed 15,000 emails (an average of 40 emails per day) per AOL member. Negative impacts of AOL's spam filtering policy on email reliability as reported in Internet forums will be addressed below.

Direct Impacts of Spam

Impacts of the spam load are quite diverse, ranging from economic impacts to psychological effects.

Economic effects have been investigated, among others, by Ferris Research. In a 2002 study they estimate the financial damage caused by spam to be around 8.9 billion USD for U.S.-American companies and around 2.5 billion USD for European companies. The damage for U.S.-American and European ISPs (Internet Service Providers) has been estimated to be around 500 million USD. When calculating the loss of productivity only, Marten Nelson of Ferris Research assumed that deleting single spam-messages would take around a second; further time may be needed if spam is not immediately recognized as such and if emails classified as spam (so-called false-positives) have to be researched in corporate mail archives. Assuming in average 4.4 seconds work per spam mail adds up to annual loss of productivity worth 4 billion USD for U.S.-American companies only.

A more practical cost example is provided by Fallows (2003), quoting a correspondent in a spam-related survey:

"I am an enterprise systems consultant who is being engaged more and more frequently to provide measures to protect against spam... [...] A tremendous amount of money is spent both in paying for my services, as well as equipment costs. Considering that the design and implementation of such a system is likely to be a minimum of four weeks of work (~\$5000/wk), and require two moderate powerful servers (~\$4000/ea), that is a cost of \$28,000." (p. 22).

Psychological effects have been investigated by the Pew Internet & American Life project. Fallows (2003) reports that 25% of the users surveyed say they reduced their use of email because of spam and an increasing number of users fear they cannot retrieve their email because of the additional spam load that now comes along with genuine email. Findings of Fittkau and Maaß' (2004) online survey seem to support some of these impressions.

Primary effects of anti-spam measures and how they are accomplished

A broad range of anti-spam measures have been developed and widely deployed in order to fight spam. The primary, intended effect of deploying anti-spam measures is a reduction of the (visible) amount of spam.

In this section, we provide a brief overview regarding the two main anti-spam approaches. The section is not intended as a detailed introduction to anti-spam technologies as such information can be found elsewhere (e.g., Graham 2002).

Typically, anti-spam measures are technical measures that are applied on the mail transportation level, i.e., they are applied either during delivery from the sender's mail server to the recipient's or during delivery from the recipient's mail server to the recipient's desktop computer.

Two main anti-spam approaches can be distinguished:

1. Filtering² emails based on specific characteristics of the content of emails.
2. Blocking email delivery if delivery attempts originate from suspicious mail servers. Blocking implies that the content of the emails to be delivered is not investigated.

Depending on the technology used, corresponding tools may be installed on the user's desktop computer or need to be implemented on the mail server used to receive mail. Some products implement combinations of different filtering and learning techniques (see Metz 2003 for an overview). Kaspersky Anti-Spam ISP Edition, for example, uses a combination of linguistic analysis, formal analysis of message characteristics and blocking based on blacklists and whitelists (Kaspersky 2003).

Filtering

Filtering targets the information contained in the body of a mail message (the part of a message users normally see) or the information contained in the message header (mostly

²Filtering in the sense of removing unwanted items from a set of items.

information used to transport the message but also From: and Subject: information).

Based on the knowledge that spam messages often carry similar content, it is possible to develop spam filters removing messages containing terms that are typical of spam messages (see, for example, FTC 2003). Examples of such terms would be "free porn", "XXX", "Warez" or "Get rich quick".

Spam filters may also target the origin of a message. If spam is sent through mail servers that are known to be operated by spam-friendly companies, then this knowledge can be used to filter these spam messages. Spam messages may also show features that are characteristic of spammers trying to disguise the origin of their messages.

Learning spam filters can be fed new examples of spam that have not been filtered yet. The filter then extracts unusual terms and uses them to identify further incarnations of the same or similar spam. Statistical spam filters (e.g., Graham 2002) calculate the probability that an email is a spam message based on occurrences of certain terms and whether these terms appeared in previous spam messages.

Blocking

A different approach to fighting spam is blocking mail delivery during the delivery process when mail servers assumed to be "suspicious" are trying to deliver messages. Blocking means a mail server refuses to accept mail from certain other servers, often according to "black lists" shared on the Internet. Blocking approaches can use IP addresses, domain names and other information provided during the delivery "handshake" between mail servers.

Lists of suspicious mail servers are shared on the Internet. Services, such as the Spamhaus Block List, allow mail servers to check *in real time* if a server trying to deliver email has earned a spammer reputation. The Spamhaus Project (2003b), the organization hosting the above mentioned list, describes their block list as follows: "The Spamhaus Block List (SBL) is a real time database of IP addresses of static spam-sources, including known spammers, spam operations and spam support services."

Secondary effects of anti-spam measures and how they manifest

The primary --intended-- effect of deploying anti-spam measures is a reduction of the (visible) amount of spam. However, there are also secondary effects which have not yet received the attention they deserve.

Fallows (2003) reports that 30% of email users are concerned their email filters might filter genuine incoming email. 23% of users are concerned email they send to others may be filtered.

In what follows, we discuss secondary effects of filtering and blocking separately as there are considerable differences.

Spam filtering: secondary effects

In general, anti-spam filters seem to perform reasonably well. Typical measures of the effectiveness of spam filters, such as the number of false-positives (genuine mail classified as spam), indicate few problems (see Metz 2003 for some empirical data).

Two infamous examples from the literature illustrate what may happen if technological measures "misjudge" the content of messages. The first example is the filter software SurfWatch having blocked access to the White House home page because text on the site contained the term "couples" (e.g., CNet 1996). The idea was that the software would prevent children from accessing inappropriate content but the software also blocked legitimate content. The second example is members of the British parliament not having received documents relating to the "Sexual Offenses Bill" under discussion (Heise Online News, 2003). Assumed to be porn, corresponding messages had been filtered by anti-spam filters installed on the parliament's mail servers.

Fallows (2003) quotes further anecdotal evidence: "The email program that I use allows me to set up email filters and prevent junk/adult email from even coming into my email inbox. But, what I have come to notice is that real emails that I need are being sent to my junk email box so I have to sort through it regardless. I found messages from clients and potential clients, my husband, and friends in the junk email." (p. 23).

In an online discussion forum (Heise Online Forum 2004) about AOL's (2003) above mentioned figure of 500 billion blocked emails, a number of contributors complained their legitimate email to AOL members was blocked as well, meaning they could not contact AOL members via email.

Considering these and other incidents (see below for further examples) it is reasonable to conclude that anti-spam filters are causing problems not be underestimated. The widespread deployment of anti-spam filters means that legitimate email may be discarded just because the sender's terminology resembled "spam terminology".

To sum up, anti-spam measures are having an impact on the language permissible in email communication.

Spam blocking: secondary effects

The primary objective of using blocking techniques is reducing a mail server's intake of messages likely to be classified as spam anyway. Messages are not checked though; they are assumed to be spam as they originate from suspicious sources.

There is quite a bit of evidence that blocking not only reduces the spam intake but also undermines reliability of email communication.

Varghese (2003) reports the following recent incident: "AOL says it is blocking email from Telstra's BigPond users because it has received complaints from its subscribers about spam being sent to them from BigPond addresses. Company spokesman Nicholas Graham said

AOL had been [...] essentially compiling a whitelist of IPs from which mail would be allowed to reach AOL users." This means AOL blocked a significant part of a whole continent's email!

Other services are blocking email servers by country of origin. Spam-filtering service SpamStopsHere, for example, mentions in the "features" section of its web site that the service "[b]locks entire countries notorious for sending spam, e.g. China and Brazil." (SpamStopsHere 2003). On a page illustrating the service's capabilities, SpamStopsHere recommends blocking Argentina, Brazil, Hong Kong, Malaysia, Nigeria, Russia, Thailand, and Singapore. Blocking China, Korea and Taiwan is even "Highly recommended".

Further anecdotal evidence comes from comments posted by system administrators and 'regular' users to Usenet newsgroups dealing with email abuse. According to these comments, it is common practice to block email originating from a number of countries and/or to filter messages based on criteria, such as the character set used (certain character sets are specific to certain countries or regions).

Most blockings are based on information coming from "black lists" shared on the Internet. The Spamhaus Project (2003) being a major host of such a black list addresses adverse effects as such: "Can the SBL block legitimate email? The SBL's primary objective is to avoid 'collateral damage' while blocking as much spam as possible. However, like any system used to filter email, the SBL has the potential to block items of legitimate email if they are sent from an IP under the control of a spammer or via IPs belonging to spam support services. The chances of legitimate email coming from such IPs are slim, but need to be acknowledged."

Contrary to Spamhaus Project's (2003) impression, there seems to be quite a bit of "collateral damage" caused by the usage of black lists. A recent discussion in the newsgroup news.admin.net-abuse.blocklisting, comprising more than 100 statements, indicates that there are quite different opinions regarding accountability and reliability of blocklists (see Blue 2003 for details). There is an abundance of requests to be removed from block lists posted to the net-abuse related newsgroup news.admin.net-abuse.blocking (see, for example, Rodriguez 2003). Often, these requests are coming from businesses renting IP blocks from major ISPs. Even though these businesses do not spam themselves, they are blocked because their ISPs have a spam history or previous owners of their net blocks were spammers. Gaudin and Gaspar (2001) quote figures suggesting that using one particularly unreliable blacklisting service was found to cause 34% false positives, i.e., genuine email classified as spam.

Cole (2003) provides a detailed overview as to why mail servers located in the net block (or IP range) of "innocent" businesses may become 'collateral damage' and how these businesses may address the situation.

Anti-Spam Measures and the Digital Divide

Although largely based on anecdotal evidence, the previous section strongly suggests that anti-spam measures are undermining reliability and usability of email in a profound way.

In this section, we look at different ways how impacts of anti-spam measures manifest and explore who might be affected most by these rather unexpected effects.

E-mail is widely regarded as one of the most important services provided by the Internet. In the U.S., for example, almost all Internet users use email which seems to be rapidly becoming more used than the telephone (Hawthornthwaite and Wellman 2002, p. 6).

The usual meaning of the term digital divide refers to inequality of access to the Internet (Castells 2001, p. 248). The term is not only used to describe differences of global scale, such as differences in access between developed countries and under-developed countries.

Castells (2001, p. 265) maintains that the gap in productivity, technology, income, social benefit, and living standards between the developed and the developing world increased during the Nineties, in spite of spectacular growth in certain areas. When trying to explain the increase Castells argues that "[...] under the current social and institutional conditions [...] the new techno-economic system seems to induce uneven development, simultaneously increasing wealth and poverty, productivity and social exclusion, with the effects being differentially distributed in various areas of the world and in various social groups. And because the Internet is at the heart of the new socio-technical pattern of organization, this global process of uneven development is perhaps the most dramatic expression of the digital divide."

Within the U.S., differences in access showing, for example, that rural and poor populations are under represented in Internet access and use have also been described as digital divide (e.g., Hawthornthwaite and Wellman 2002).

Exploring Internet access in the U.S., Servon (2002, p. 4) argues that policy makers and the media have thus far defined the digital divide narrowly and incompletely by focusing on access in terms of possession or permission to use a computer and the Internet. Challenging this conception of the problem, Servon argues that deep divides remain although under represented groups are making dramatic gains. In particular, Servon argues that deep divides remain between those who possess the resources, education, and skills to reap the benefits of the information society and those who do not. An different view is provided by Compaine (2000) arguing that there was a digital divide in the 1990s but that by 2000 the gaps were rapidly closing.

Our findings suggest that anti-spam measures may contribute to the digital divide in at least two distinct areas. Both are yet to receive the scientific attention they deserve.

What happened to my email?

Local impacts of spam blocking/filtering

First, anti-spam measures may further contribute to the excluding of those who lack the knowledge and/or education to understand what happened if their email did not get through (for both sender and recipient). A related issue is understanding what could be done such that the problem won't occur again.

This kind of exclusion is basically location-independent and may occur in the U.S. just as well as in under-developed countries. It is more likely, however, to occur in areas of lower education which are often areas of lower income too. The NTIA (1999) report states that for the U.S., the digital divide is widening at lower income levels.

Low income may further contribute to widening the digital divide as being able to afford the "right" kind of Internet access may be a crucial aspect. ISPs offering Internet access at discount rates often lack quality support staff, thus requiring customers to solve their problems on their own. Such ISPs also tend to lack sufficiently staffed "abuse desks" which means these ISPs may end up being blocked by more responsible ISPs. Considerable technical expertise may be a prerequisite to using these ISPs. Depending on the region, cost of connection may differ considerably. Servon (2002, p. 43) mentions that monthly Internet access charges are only 1.2 percent of the average monthly income in the U.S. but they are 80 percent of the average monthly income in Buthan and 278 percent of the average monthly income in Nepal.

Another aspect to consider is the location of Internet access points and the costs associated with accessing them. In certain geographical areas, such as rural areas or lower-income areas, the number of access points maintained by ISPs may be limited, thus leaving not much choice to those who rely on using access points that are within reach of a local call.³ This means that customers who do not have a choice may face the problems discussed above. This again is hurting the most those coming from lower income/education backgrounds who cannot afford paying premium rates for Internet access or hiring specialists for helping them with setting up alternate Internet connections. Using "external" web-based email services, such as Hotmail or Yahoo, is not always a solution.

Sorry, you are living in the wrong country:

Global impacts of spam blocking/filtering

Second, in the long term, anti-spam measures may lead to the excluding those who are located in countries not able or not willing to prevent spamming. As anti-spam legislation is getting tougher in countries, such as U.S. and Australia, spam will increasingly be sent from or relayed in developing countries.

³ In many countries, cost of a phone call depend on the physical distance between caller and callee. "Local call" usually means reduced cost.

As mentioned before, there is some evidence that whole networks and/or blocks of IP addresses located in specific countries get blocked by services located in the "developed" world. The reason for the apparently widespread blocking seems to be that enterprises operating mail servers in developing countries often do little to prevent abuse of their servers for spam purposes. A number of large ISPs in developing countries have a track record of hosting spam services. Some system operators may not be aware of the abuse of their systems. For example, the author received porn spam being relayed by the mail server of a Korean elementary school!

Businesses in certain geographic areas may be blocked as well. Maglio (2003) describes how their company relies on services provided by a large ISP and how they got into trouble because of the ISP being black-listed (and therefore widely blocked) for their lack of engagement against spamming customers.

There is anecdotal evidence that customers experiencing problems with their own ISP may be forced to pay for accessing properly working mail servers. This development was described by Ercolessi (2003) in a discussion about problems with the infamous Italian ISP interbusiness.it. According to information posted to the international net-abuse newsgroup news.admin.net-abuse.mail, interbusiness.it is widely known (and blocked) for harboring spammers. Checking with the Spamhaus Advisory list reveals that in January 2004, the Spamhaus Advisory lists fifty entries for internetbusiness.it, among them entries existing for more than a year. This means that a lot of interbusiness.it customers cannot use their interbusiness.it IP addresses for hosting mail servers as mail from these addresses would be blocked by ISPs making use of block lists like the Spamhaus Advisory. Ercolessi (2003) writes "The most savvy of IT managers know by now that Interbusiness has no abuse desk, that a large part of the world blocks their IP space, and for this reason they often buy mail services elsewhere, but STILL buy Interbusiness connectivity on purely economical grounds." (Ercolessi 2003). Interbusiness bandwidth is then used for other purposes than sending email, such as web surfing and downloading. There are other ways for circumventing those problems. Referring to his own study on the Russian Internet, Castells (2001, p. 263) reports that "Russian banks and foreign international business linked the main Russian centers to the world with specific telecommunications links, largely bypassing the obsolete Russian telecommunications infrastructure".

It is important to keep in mind that in most countries, ordinary citizens won't have such opportunities.

Summary and future research

This paper provides two main contributions to the discussion of the spam and anti-spam measures.

First, we have motivated that while providing considerable benefit, anti-spam measures, such as filtering and blocking, also create specific problems. Although

largely based on Internet material and anecdotal evidence, our findings clearly indicate that anti-spam measures are undermining reliability and usability of email in a profound way. Put in a nutshell, reliably working email is no longer a question of technically efficient and effective email transportation as it used to be (and as it should be--cf. regular mail). Legitimate email may be rejected or dumped just because the sender's terminology resembled 'spam terminology' or because the email was sent through a 'suspicious' email server.

The sources we reference largely result from the speed at which the spam problem has emerged and the occupation of the key players who are often employed as technical staff or system administrators. Also, we are not aware of any study addressing aspects of these problems in a more systematic way. There are studies regarding the technical performance of anti-spam measures, such as the percentage of false-positives, but these studies do not address the secondary impacts we are interested in.

The second main contribution of this paper is framing the impacts of anti-spam measures in the context of the digital divide. Departing from the point of view that the digital divide is not only about possession or permission to use a computer and the Internet but also about resources, education, and skills, we motivated that most likely, the impacts of anti-spam measures are hurting most those who are disadvantaged already.

Clearly, our findings relating to the digital divide are preliminary and need to be explored in more systematic way. As an exploratory study, however, we believe the paper serves its purpose as it describes the situation and surveys key terms, key resources and key players. Most importantly, the study indicates areas that need to be researched in more detail.

We proceed with analyzing the situation in Darwin which is located at Australia's tropical top end. Darwin is one of Australia's capital cities. Due to its isolated location, the city provides an interesting environment to investigate urban, rural and remote issues at the same time. We are looking at the different ways of accessing the Internet in Darwin and surrounding rural and remote areas. We explore how these options can be utilized (e.g., local call or long distance call; time limits), and whether any of the Internet Service Providers within reach are listed on block lists.

References

- Aberdeen Group (2002). 2003: Predictions for Security and Privacy. Available at URL <http://www.aberdeen.com/ab%5Fcompany/researchareas/security2003.htm> (last accessed 12/30/03).
- AOL (2003). America Online Releases 'Top 10 Spam' List of 2003. Press release published 12/31/03 is available at URL http://media.aoltimewarner.com/media/press_view.cfm?release_num=55253692 (last accessed 01/05/04)
- Baseley, W. D. (1998). The Email Abuse FAQ (last updated June 25, 1998) Article available at URL <http://members.aol.com/emailfaq/emailfaq.html> (last accessed

- 12/30/03). The FAQ can also be found in the Usenet newsgroups news.admin.net-abuse.email and news.answers.
- Blue, T.M. (2003). Blocklists Accountability, Standards, Who is Policing Blocklists. Posting to the Usenet newsgroup news.admin.net-abuse.blocklisting on 12 Aug 2003. Message-ID: <65ab995e.0308121542.4bccaede@posting.google.com>
- Castells, M. (2001). *The Internet galaxy. Reflections on the Internet, Business and Society*. Oxford University Press.
- Center for Democracy and Technology (n.d.). Spam, Unsolicited Commercial Email, Junk Email. Available online at URL <http://www.cdt.org/speech/spam/> (last accessed 01/06/2004).
- CNet (1996). SurfWatch to Give Users More Control. CNet News. Article available at <http://news.com.com/2102-1023-211137.html> (last accessed 02/15/03).
- Cole, W.K. (2003). Blacklists, Blocklists, DNSBL's, and survival: How to Survive as a Non-Combatant Emailer in the Spam Wars. A collection of frequently asked and too-often poorly answered questions. URL <http://www.sconsult.com/bill/dnsblhelp.html> (last accessed 01/02/04).
- Compaine, B.M., editor (2000). *The Digital Divide. Facing a Crisis or Creating a Myth?* MIT Press, Cambridge, MA.
- Cranor, L. and LaMacchia, B. (1998). Spam! *Communications of the ACM* August, Volume 41, No 8, pp. 74-83.
- Ercolossi, F. (2003). Re: interbusiness.it? Posting to the Usenet newsgroup news.admin.net-abuse.email on Feb 10 2003. Message-ID <b296sr\$2ivh\$1@half.spin.it>.
- Fallows, D. (2003). Spam. How it is Hurting Email and Degrading Life on the Internet. Report published October 22, 2003 by the Pew Internet & American Life project. Washington, DC, USA. URL <http://www.pewinternet.org>.
- Ferris Research (2003). <http://www.ferris.com>.
- Fittkau and Maaß (2004). Ergebnisse der 18. WWW-Benutzer-Analyse (1. April bis 5. Mai 2004). URL <http://www.w3b.de>.
- FTC (2003). False Claims in Spam. A report by the U.S. Federal Trade Commission's Division of Marketing Practices. Released April 30, 2003. Available online at <http://www.ftc.gov/reports/spam/030429spamreport.pdf> (last accessed 01/13/03)
- Gaudin, S. and Gaspar, S. (2001). The Spam Police. Tactics Used by Self-Appointed Spam Fighters Come Under Fire. *Network World*, 09/10/01 Available at URL <http://www.nwfusion.com/research/2001/0910feat.html> (last accessed 12/30/03).
- Geer, D. (2004). Will New Standards Help Curb Spam? *IEEE Computer* February, pp. 14-16.
- Graham, P. (2002). Will filters kill spam? Available at URL <http://www.paulgraham.com/wfks.html> (last accessed 04/30/2003). The web article is derived from an article by the same author published in the January 2003 issue of the *Computer Security Journal*.
- Heise Online Forum (2004). http://www.heise.de/newsticker/foren/go.shtml?list=1&forum_id=51255
- Heise Online News (2003). Spam-Filter verärgert britische Abgeordnete. Available at URL <http://www.heise.de/newsticker/data/wst-09.02.03-003/> (last accessed 02/09/03).
- Haythornthwaite, C. and Wellman, B. (2002). The Internet in Everyday Life. An Introduction. In: Wellman, B. and Haythornthwaite, C. (eds.) *The Internet in Everyday Life*. The Information Age Series. Blackwell Publishing, Malden, MA.
- Kaspersky (2003). Kaspersky Labs Now Battling Spam at the ISP Level. Product announcement released 12/30/2003.
- Lueg, C. (2003). Spam and Anti-Spam Measures: A Look at Potential Impacts. *Proceedings of the Informing Science & IT Education Conference (IS 2003)*. Pori, Finland, June 2003.
- Maglio, R. (2003). Innocent casualty of Spews. Posting to the Usenet newsgroup news.admin.net-abuse.blocklisting on 13 Aug 2003. Message-ID <313f98de.0308130801.69118996@posting.google.com>
- Metz, C. (2003). Corporate Antispam Tools. *PC Magazine*. Available at URL <http://www.pcmag.com/article2/0,4149,849390,00.asp> (last accessed 02/16/03)
- Mueller, S. H. (2003): What is Spam? Article available at <http://spam.abuse.net/overview/whatisspam.shtml> (last accessed 01/13/03).
- NOIE (2002). Final Report of the Australian National Office for the Information Economy (NOIE) review of the spam problem and how it can be countered. Report available at http://www.noie.gov.au/projects/confidence/Improving/Spam/Interim_Report/contents.htm (last accessed 05/03/2003).
- NTIA (1999). Falling Through the Net: Defining the Digital Divide. Report published by the U.S. Department of commerce, National Telecommunications and Information Administration. Available online at URL <http://www.ntia.doc.gov/ntiahome/ftn99/contents.html> (last accessed 01/06/2004)
- Rodriguez, G. (2003). SPEWS blocking a range with mine included , how to get out? Posting to the Usenet newsgroup news.admin.net-abuse.blocklisting on July 22 2003. Message-ID <b7efc7c3.0307220944.3e1a4d00@posting.google.com>
- Southwick, S. and Falk, J.D. (1998). The Net Abuse FAQ. <http://www.cybernothing.org/faqs/net-abuse-faq.html> (last accessed 12/30/03).
- SpamStopsHere (2003). <http://www.spamstopshere.com/> (last accessed 05/03/2003).
- The Spamhaus Project (2003). The Spamhaus Block List (SBL) Advisory FAQ. Available at URL <http://www.spamhaus.org/sbl/sbl-faqs.lasso> (last accessed 01/13/03).
- Varghese, S. (2003). AOL blocking BigPond mail because of spam. *The Sydney Morning Herald* 04/30/2003.
- Servon, L.J. (2002). *Bridging the digital divide*. The Information Age Series. Blackwell Publishing, Malden, MA, U.S.A.