Journal of Economic Perspectives—Volume 26, Number 3—Summer 2012—Pages 87–110

The Economics of Spam

Justin M. Rao and David H. Reiley

The term "spam," as applied to unsolicited commercial email and related undesirable online communication, is derived from a popular Monty Python sketch set in a cafe that includes the canned meat product SPAM in almost every dish. As the waitress describes the menu with increasing usage of the word "spam," a group of Vikings in the cafe start singing, "Spam, spam, spam, spam, spam," drowning out all other communication with their irrelevant, repetitive song. The analogy to unsolicited commercial solicitations jamming one's inbox seems apt. Every day about 100 billion emails are sent to valid email addresses around the world; in 2010 an estimated 88 percent of this worldwide email traffic was spam (Symantec 2010; MAAWG 2011). Almost all of this spam is illegal under current laws.

How does spam differ from legitimate advertising? If you enjoy watching network television, using a social networking site, or checking stock quotes online, you know that you will be subjected to advertisements, many of which you may find irrelevant or even annoying. Google, Yahoo!, Microsoft, Facebook, and others provide valuable consumer services, such as search, news, and email, supported entirely by advertising revenue. While people may resent advertising, most consumers accept that advertising is a price they pay for access to content and services that they value. By contrast, unsolicited commercial email imposes a negative externality on consumers without any market-mediated benefit, and without the opportunity to opt out.

This negative externality makes spam particularly useful for teaching purposes. When asked for an example of an externality, most economists think of environmental

■ *Justin M. Rao is a Research Scientist, Microsoft Research, New York, New York. David H. Reiley is a Research Scientist, Google, Inc., Mountain View, California. When this paper was written, both authors were working at Yahoo! Research, Santa Clara, California.*

http://dx.doi.org/10.1257/jep.26.3.87. doi=10.1257/jep.26.3.87

pollution: groundwater toxins, acid rain, air pollution, global warming, and so on. Indeed, given the great linguistic generality of the term "pollution" (including noise pollution, light pollution, and others), it can be difficult for economists to find an example of a negative externality that *cannot* be described as a form of pollution. Our two favorite nonpollution externalities for teaching are traffic congestion and spam.

Of course, a similar externality has been present for decades in other forms of unsolicited advertising, including junk mail, telemarketing, and billboards. These intrusive activities also impose claims on consumer attention without offering compensation or choice. However, email spam is breathtakingly larger in magnitude, with quantities in the absence of automated spam filters equal to hundreds of emails per user per day—if our email inboxes stood unguarded, they would quickly become totally useless. (In contrast, junk mail has not yet reduced our unguarded postal mailboxes to this fate.) One can purchase unsolicited email delivery on the black market for a price at least a thousand times less than that to send bulk postal mail. Spam has become such a widespread phenomenon that trademark holder Hormel finally stopped objecting to the use of the term to refer to unsolicited email (Templeton, undated).

Spam also seems to be an extreme externality in the sense that the ratio of external costs to private benefits is quite high. We estimate that American firms and consumers experience costs of almost $20 billion annually due to spam. Our figure is more conservative than the $50 billion figure often cited by other authors, and we also note that the figure would be much higher if it were not for private investment in anti-spam technology by firms, which we detail further on. On the private-benefit side, based on the work of crafty computer scientists who have infiltrated and monitored spammers' activity (Stone-Gross, Holz, Stringhini, and Vigna 2011; Kanich et al. 2008; Kanich et al. 2011; Caballero, Grier, Kreibich, and Paxson 2011), we estimate that spammers and spam-advertised merchants collect gross worldwide revenues on the order of $200 million per year. Thus, the "externality ratio" of external costs to internal benefits for spam is around 100:1.

In this paper, we start by describing the history of the market for spam, highlighting the strategic cat-and-mouse game between spammers and email providers. We discuss how the market structure for spamming has evolved from a diffuse network of independent spammers running their own online stores to a highly specialized industry featuring a well-organized network of merchants, spam distributors (botnets), and spammers (or "advertisers"). Indeed, email service provision has become more concentrated in part because the high fixed costs and economies of scale of filtering spam offer a significant advantage to large service providers. We then put the spam market's externality ratio of 100 into context by comparing it to other activities with negative externalities, such as pollution associated with driving an automobile, for which we estimate a ratio of about 0.1, and for nonviolent property crime such as automobile theft, for which we estimate a ratio of 7–30. Lastly, we evaluate various policy proposals designed to solve the spam problem, cautioning that these proposals may err in assuming away the spammers' ability to adapt.

The History of Spam: Cat-and-Mouse Games

Email is sent via a "sender push" technology called Simple Mail Transfer Protocol (SMTP). Other examples of sender-push transfer include postal mail, text messaging, and voice mail. (In contrast, the Hypertext Transfer Protocol (HTTP) used in web browsing is "receiver pull"—nothing shows up in your web browser until you specify a URL.) SMTP was designed in the early 1980s when the trust level across what was then called the "Arpanet" was quite high. Accordingly, senders were not required to authenticate their emails. SMTP servers all over the world were programmed to cooperate in relaying messages. In many respects, SMTP replicates the "transfer protocol" of the U.S. Postal Service. Anyone in the United States can anonymously drop a letter in a mailbox and, provided it has proper postage, have it delivered, without any requirement for the sender to provide an authentic return address.

Spammers first developed technology to automate the sending of bulk email in the mid 1990s by opportunistically tapping into mail relay servers and anonymously floating a deluge of spam from phony domains (Goodman, Cormack, and Heckerman 2007). In 1994, the attorneys Canter and Siegel hired a programmer to automate a posting to every USENET newsgroup in existence, so that thousands of discussion groups devoted to every topic from *Star Trek* to board games were inundated with advertisements for services to help immigrants apply for the green-card lottery. This software soon evolved into the first automated bulk emailer (Zdziarski 2005, pp. 10–13). In 1995, the first commercial "spamware," aptly titled Floodgate, appeared for sale at a price of $100. Floodgate advertised its ability to harvest email addresses from a variety of sources including newsgroups, CompuServe classified ads, AOL Member Directory, and other sources. Then, via the included companion software Goldrush, it promised an ability to send out thousands of emails per hour (Zdziarski 2005, p. 16; Everett-Church 1999). Such software, crude by today's standards, enabled spammers to send email at a cost on the order of $0.0001 per message. Since then, the spam market has been shaped by the technological cat-and-mouse game between spammers and email service providers.

Anti-spam Filtering Techniques

As an early response to spam, Internet administrators developed authentication protocols: where previously one only had to type a password to collect one's incoming mail, now most had to authenticate themselves by providing a password to send outgoing mail. To prevent domain spoofing—using the domain of a well-known company to make an email seem more legitimate—domain authentication routines check that the IP address listed in the Domain Name System matches the sending IP. However, many SMTP servers remained unauthenticated for a long time, and the default mail delivery protocol is still to deliver email from any sending IP address.

After authentication, the arsenal of filtering technologies consists of machine learning, crowdsourcing, and IP blacklisting. Such screening devices detect suspected spam messages and either reject them from being delivered, or send them to a junk-mail folder.

The machine-learning approach dates from the late 1990s (Sahami, Dumais, Heckerman, and Horvitz 1998; Androutsopoulos, Koutsias, Chandrinos, Paliouras, and Spyropoulos 2000). A typical machine-learning implementation uses "ground truth" data on a subset of observations to learn rules to classify the remaining data. With spam, the ground truth is given by human-labeled examples of spam versus non-spam emails and the algorithm is trained to recognize features of the email that predict whether it is spam. For example, one can have the classifier examine the predictive power of all words and word pairs in the subject lines of the emails, which might lead to dummy variables for the presence of "Viagra," "Nigeria," and "Free Money" being included as key predictors. Other examples of heavily weighted features include unusual punctuation common to spam, such as "!!!", and nouns associated with spam-advertised products, such as "Rolex". Every URL contained in a message could also be treated as a possible predictor as spam emails nearly always include the URL of the website to place orders for the advertised product. Any machine-learned filter can have false positives—that is, legitimate mail that is filtered to the junk folder (for instance, spam filters might make it hard to converse legitimately about bank transfers in Africa).

Spammers responded with creative misspellings designed to avoid the filters, such as "V1agra," created many unique URLs all mapping to the same order form, and included attachments of graphical images of text messages, which became popular with spammers when they realized that text-based classifiers could not find the text in the form of a GIF or JPEG image. Spammers also include irrelevant text passages, such as excerpts of news stories that are common in legitimate conversations, or create random permutations of words from one email to the next to throw classifiers off track. Of course, over time the anti-spam classifiers continued to improve and adapt, too. Goodman, Cormack, and Heckerman (2007) present a nice introduction to such anti-spam technology for nonexperts.

Crowdsourcing represents a way to collect additional data to improve the predictive power of machine-learning models. Large webmail providers such as Yahoo! Mail collect data when users press the "mark as spam" button to move email from the inbox to the junk mail folder. Data from such marked spam can be used, as soon as that same day, to retrain the spam classifier. However, most users just delete irrelevant emails rather than marking them as spam. We took a random sample of six months of mail activity for 1.3 million active Yahoo! Mail users and found that only 6 percent of users ever marked any email as spam, but the vast majority deleted messages without reading them.

Spammers have developed a strategic response to the spam voting system. In addition to the "spam" button in the inbox, webmail services also provide a "not spam" button to mark false-positive messages in the junk mail folder. In four months of 2009 Yahoo! Mail data, our Yahoo! colleagues found that (suspiciously) 63 percent of all "not spam" votes were cast by users who never cast a single "spam" vote. After examining additional data on these accounts, such as IP address, position in the network of users, and repeatedly casting not-spam votes on a variety of emails that were receiving multiple "spam" votes from legitimate users, the authors concluded

that the vast majority of these accounts were created by spammers to cast strategic votes in order to help their campaigns beat the spam filters (Cook, Hartnett, Manderson, and Scanlan 2006; Ramachandran, Dasgupta, Feamster, and Weinberger 2011). The researchers discovered 1.1 million of these sleeper accounts, and Yahoo! inserted a detection algorithm to mitigate the effects of this strategic voting.

The single most effective weapon in the spam-blocking arsenal turns out to be blacklisting an email server (Cook, Hartnett, Manderson, and Scanlan 2006; Ramachandran, Feamster, and Vempala 2007). In 2011, 80 percent of all emails received by Yahoo! Mail were rejected by their servers through IP blacklisting. Fortunately, just as the postmark from the sending post office limits the ability to spoof one's return address, Transmission Control Protocol (TCP) makes it impossible to spoof the IP address of the mail server from which the message was sent. Therefore, if email administrators noticed that their users were receiving tremendous amounts of mail from one server, they could "blacklist" such a server. Sharing blacklist information enables multiple organizations to shut down spam activity more quickly. For example, the Spamhaus Block List, founded in 1998 by Steve Linford, now protects nearly 1.8 billion email inboxes from spam (⟨http://www.spamhaus.org/organization/index.lasso⟩, accessed February 9, 2012).

An unintended side effect of blacklisting occurs when a single user starts sending spam and causes their email server to be blacklisted. At that point, everyone else using the same email server will suddenly find their outbound emails being blocked. This situation could arise within any large organization, like a college, a corporation, or a shared Internet service provider (ISP). Of course, information technology professionals can then sort out the problem, and organizations such as Spamhaus strive to act quickly in unblocking any email server who was falsely accused or who corrects the problem with its users, but blacklists still routinely cause reliability problems for users trying to send email.

The larger email services such as Yahoo! Mail, Microsoft Hotmail, and Google Gmail have large, dedicated anti-spam and customer support teams. The high fixed costs of anti-spam technologies and benefits of crowdsourced data have made it difficult for small email providers to compete, which has contributed to significant increases in concentration in email provision since the mid 1990s. We obtained market share data (from comScope) for the top 50 largest consumer web-based email services (including home Internet service providers) for the period 2006–2012. The data show that webmail provision has become increasingly concentrated in the "Big Three" of Hotmail, Yahoo! Mail, and Gmail. The three-firm concentration ratio in this market has increased from 55 percent to nearly 85 percent over the last six years; we believe that spam is a significant contributor to this increase in concentration.

Botnets

Blacklists gradually made it impossible for spammers to use their own servers (or others' open relay servers) with fixed IP addresses. Spammers responded with a "Whack-a-Mole" strategy, popping up with a new computer IP address every time the old one got shut down. This strategy was observed and named as early as 1996, and

eventually became considerably cheaper with another major innovation in spam: the botnet.

A botnet is a network of "zombie" computers infected by a piece of malicious software (or "malware") designed to enslave them to a master computer. The malware gets installed in a variety of ways, such as when a user clicks on an ad promising "free ringtones." The infected computers are organized in a militaristic hierarchy, where early zombies try to infect additional downstream computers and become middle managers who transmit commands from the central "command and control" servers down to the frontline computers (John, Moshchuk, Gribble, and Krishnamurthy 2009; Caballero, Poosankam, Kreibich, and Song 2009; Cho, Caballero, Grier, Paxson, and Song 2010).

The first spamming botnets appeared in 2003. Static blacklists are powerless against botnets. In a botnet, spam emails originate from tens of thousands of IP addresses that are constantly changing because most individual consumers have their IP addresses dynamically allocated by Dynamic Host Control Protocol (DHCP). Dynamic blacklisting approaches have since been developed; Stone-Gross, Holz, Stringhini, and Vigna (2011) document that 90 percent of zombie computers are blacklisted before the end of each day. However, if the cable company assigns a zombie computer a new IP address each day, that computer gets a fresh start and can once again successfully send out spam.

In response to botnets, many Internet service providers, such as Comcast, began to prevent their users' computers from operating as send-mail servers. This meant that individuals and small businesses could no longer run their own mail servers, as in the original, decentralized vision of the Internet, and now had to rely on larger commercial email vendors.

A second generation of botnets makes use of accounts at large commercial email providers. For example, a zombie could be programmed to sign up for hundreds of thousands of free email accounts at Gmail, and then send spam email through these accounts. Email providers have implemented sending thresholds designed to detect and prevent this sort of spamming. If a user exceeds these limits, the system may refuse to send out the email, or it may ask the user to solve a CAPTCHA (as discussed in the next subsection). Such rules cut down on outbound spam, but also impose negative side effects on users who happen to be high-volume senders of legitimate email. In 2011, Yahoo! Mail experienced an average of 2.5 million sign-ups for new accounts each day. The anti-spam team deactivated 25 percent of these immediately, because of clearly suspicious patterns in account creation (such as sequentially signing up account names JohnExample1, JohnExample2, . . .) and deactivated another 25 percent of these accounts within a week of activation due to suspicious outbound email activity.

In 2009, six botnets accounted for over 90 percent of botnet spam (Symantec 2010; John, Moshchuk, Gribble, and Krishnamurthy 2009). The largest botnet on record, known as Rustock, infected over a million computers and had the capacity to send 30 billion spam emails per day before it was taken down in March 2011. Microsoft, Pfizer, FireEye network security, and security experts at the University

of Washington collaborated to reverse engineer the Rustock software to determine the location of the command servers. They then obtained orders from federal courts in the United States and the Netherlands allowing them to seize Rustock's command-and-control computers in a number of different geographic locations. (Microsoft financially supported the operation presumably because Rustock sent its emails through Windows Live Hotmail accounts, while Pfizer participated because a Rustock spam often advertised counterfeit versions of Pfizer's patent-protected Viagra.) If the servers had been located in less-friendly countries, it is not clear whether the takedown could have been successful. The takedown of this single botnet coincided with a one-third reduction in global email spam—and hence a one-quarter reduction in global email traffic (Thonnard and Dacier 2011; Microsoft 2011). Thus, the efforts of these private firms produced a remarkably large *positive* externality.

CAPTCHA: Screening Humans from Bots

To avoid spammers setting up many commercial email accounts, services like Yahoo! Mail have implemented a screening device called a CAPTCHA, which is an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart." This test will be familiar to most readers as a set of twisty, distorted text characters. Spammers turned to visual-recognition software to break CAPTCHAs, and in response email providers have created progressively more difficult CAPTCHAS, to the point where many legitimate human users struggle to solve them.

However, the big breakthrough in CAPTCHA breaking arose when spammers figured out how to employ human labor to break CAPTCHAs for them. In this idea's first incarnation, a spammer would set up a pornography site, offering to display a free photo to any user who could successfully type in the text characters in a CAPTCHA image. In the background, their software had applied for a mail account at a site like Hotmail, received a CAPTCHA image, and relayed it to the porn site; they would obtain text from a user interested in free porn and relay this back to the Hotmail site (Kotadia 2004).

More formal labor markets subsequently developed for CAPTCHA breaking (Motoyama, Levchenko, Kanich, McCoy, Volker, and Savage 2010). A market maker typically operates one website for interacting with buyers of CAPTCHA-breaking services, and another for interacting with workers who sell their labor. For example, one can purchase CAPTCHA-breaking services from the DeCaptcher website, which transmits each CAPTCHA to a worker at the PixProfit website for breaking, then back to the customer at DeCaptcher. The customer may use a separate piece of software (such as GYCAutomator, which specializes in Gmail, Yahoo! Mail, and Craigslist CAPTCHAs) to transmit the CAPTCHA and its solution. The entire process takes less than 30 seconds. The market wage advertised for CAPTCHA-breaking laborers declined from nearly $10 per thousand CAPTCHAs in 2007 to $1 per thousand in 2009. These labor markets started with Eastern European labor and then moved to locations with lower wages: India, China, and Southeast Asia.

In February 2012, Kotalibablo.com was advertising to workers that they could earn wages starting at $0.35 per thousand. The same company operates the buyer-facing website Antigate.com, which at that time advertised a price of $0.70 per thousand to customers wanting to break CAPTCHAs. Motoyama, Levchenko, Kanich, McCoy, Voelker, and Savage (2010) measured typical response times of around 10–15 seconds per CAPTCHA, with accuracy rates around 90 percent. (During one peak-load period, they experimentally measured a labor supply elasticity of approximately one: increasing their bid amount from $2 per thousand to $5 per thousand increased quantity solved from 8 to 18 per second.) Several websites can provide more than ten CAPTCHAs per second, putting total industry capacity (at a price of $1 per thousand) at over a million broken CAPTCHAs per day. These services market themselves as "Image to Text" providers and operate in the light of day—as of 2012 U.S. law, there does not appear to be anything illegal about the services they offer.

CAPTCHAs are also used to authenticate senders in what are known as "challenge-response systems." Such a service will intercept messages from anyone not in a preset contact list, sending an autoreply before allowing the message to be delivered. The autoreply requires that the sender solve a CAPTCHA, thus authenticating the sender as human. Such systems have been available for at least seven years, but the market has for the most part rejected this technology, and with good reasons (Isacenkova and Balzarotti 2011). First, the autoreply "challenge" itself often gets caught in a spam filter because it contains stock text and a link, and is sent frequently from the same sender—which are all strong signals in machine-learned spam filters. Second, it requires that receivers maintain a continually updated contact list. Third, spammers can use the challenge-response system to spoof messages from unsuspecting "senders," who receive the spammers' message as "backscatter spam" when they fail the challenge and get bounced to the apparent sender.

Hijacking Accounts from Legitimate Users

Another recent strategy of botnets has been to hijack existing email accounts from legitimate users. (These same techniques can be used for even more nefarious purposes, such as hijacking a bank account; for more details about this form of online crime, we refer readers to Moore, Clayton, and Anderson 2009, in this journal.) For example, "phishing" occurs when the culprit sends an email posing as a legitimate institution—say, "Hotmail user account services," often including the actual logo of the institution being spoofed—and asks the victim to visit a website to "verify your account password." In the practice of "keylogging," a type of malware records keystrokes and transmits information (especially suspected passwords) to the spammer. The practice of "packet sniffing" takes advantage of small companies and colleges who still transmit user passwords over the Internet in unencrypted text, and so a spammer "listening" at a login page can not only hijack that account, but also any other accounts (such as Yahoo! Mail) for which the user has conveniently chosen the exact same password. This technique was recently used to obtain access to 93,000 accounts on the Sony Playstation Network (Gross 2011).

In 2005, an industry consortium established a technology standard called Domain Keys Identified Mail (DKIM) as a new weapon in the war against both spamming and phishing. Now adopted by a number of firms, including Yahoo! Mail, Gmail, PayPal, and eBay, this standard creates a digital signature that email senders can adopt. For example, if a phisher pretends to be PayPal asking a user to verify their account password, Yahoo! Mail will immediately notice that the message does not have the correct digital signature (based on public-key encryption) and will therefore reject the forged email without delivering it. Unfortunately, spammers have already responded to this strategy by trying to hijack the account of a corporate user that has been "whitelisted" via DKIM. In March 2011, a number of accounts became compromised at Epsilon, an email service provider who handles the sending of legitimate bulk email for a number of corporate clients, such as TiVo, Capital One, U.S. Bank, and the Kroger grocery chain (Moyer 2011).

On the whole, anti-spam efforts at large companies have mitigated the nuisance of spam to customers. However, the cat-and-mouse moves seem certain to continue.

Spammers and the Field of Dreams

From a spammer's perspective, any online platform delivering eyeballs is a natural target. In other words, as Kevin Costner's character in *Field of Dreams* famously heard, "If you build it, they will come."

Spam is prevalent on social bookmarking sites[1] (Krause, Schmitz, Hotho, and Stumme 2008) and online classifieds (Tran, Hornbeck, Ha-Thuc, Cremer, and Srinivasan 2011). On Twitter, spam takes the form of inserting a spammy link to an ongoing conversation between users (Yardi, Romero, Schoenebeck, and boyd 2009), using Twitter's hashtag feature. Twitter spam also occurs when an ostensible fan of a celebrity writes a message including the characters "@LadyGaga," in hopes of getting it exposed to her fans. Facebook suffers relatively less from spam because of the way it requires users to verify connections with each other, but spammers continue to invent new techniques, from malicious apps to friend requests from fictitious identities, that keep Facebook's anti-spam team quite busy (Warren 2011; Cohen 2012; Ghiossi 2010). Text-messaging spam has become a serious problem in certain countries: one source estimated that 30 percent of text messages in China are now spam. However, in the United States the relatively high price of SMS messaging (often $0.10 per message, orders of magnitude higher than in China) has kept text message spam rates below 1 percent (Gómez Hidalgo, Bringas, Sánz, and García 2006). Text spam is aggressively filtered by cell phone providers, especially for text messages from a computer to a phone through a webmail client (Almeida, Gómez, and Yamakami 2011). Providers of online instant message software also struggle to block spam.

Next to email spam, the most prominent form of spam is known as "web spam" or "black-hat search-engine optimization." A typical web-spam implementation mines

[1] Social bookmarking, also known as "tagging," is a way to share webpages with a community of users.

news feeds for headlines and automatically creates pages with snippets of popular stories. The article snippet is used under a "fair use" exception to copyright law, and the remainder of the page is typically saturated with advertisements. Such web spam can deceive search engines into featuring these ad-laden pages prominently in search results about popular topics, thereby annoying users, but it is not illegal. It differs fundamentally from all the other forms of spam discussed in this paper in that it is not sender-push: One only sees a web spam page if one voluntarily clicks. Web spam has been combated through machine learning about the credibility of potential links and the downgrading of low-credibility links in search results (Caverlee and Liu 2007; Zhou, Burges, and Tao 2007; see also Ntoulas, Najork, Manasse, and Fetterly 2006, and Castillo, Donato, Gionis, Murdock, and Silvestri 2007).

Market Structure

Most spam is illegal under the United States CAN-SPAM Act of 2003, which requires unsolicited emails to have valid return addresses and opt-out provisions. While many people use "spam" to refer to the (sometimes annoyingly frequent) messages they receive from businesses with which they have previously transacted, for the purposes of this paper we define spam to be messages from economic agents who do not have a previous relationship with the customer and who do not offer opt-out provisions.

The spam market does have some similarities to the market for legitimate online advertising (whose institutions have been described in this journal by Evans 2009) in the sense that spam attempts to generate a sale. However, while in legitimate advertising the whole point is to promote awareness (of a firm or a product), spam typically uses obfuscation to get its message through. Spam-based advertising is dominated by "affiliate marketing," in which a merchant recruits intermediaries known as affiliates (a.k.a. spammers) to advertise on its behalf, in return for a share of the final purchase amount (Levchenko et al. 2011; Samosseiko 2009; Kanich et al. 2011; Kanich et al. 2008). Thus, a merchant advertising via spam generally shrouds its identity, hiding behind an array of cookie-cutter storefronts, in order to increase the chances of getting its offer through to users.

The supply (or "publishing") side of the spam market has become dominated by botnets, as discussed earlier. Several teams of computer scientists have demonstrated that botnets are distinct economic entities from the merchants on the demand side of the spam market (John, Moschuk, Gribble, and Krishnamurthy 2009; Kanich et al. 2011; Stone-Gross, Holz, Stringhini, and Vigna 2011). Major merchants are advertised by multiple botnets, and botnets compete with each other for clients (Thonnard and Dacier 2011). A botnet may either rent out its services to independent spammers, or send its own spam while acting as an affiliate for a merchant. Both business models appear to be widely practiced (John, Moschuk, Gribble, and Krishnamurthy 2009; Kanich et al. 2011; Stone-Gross, Holz, Stringhini, and Vigna 2011). The market structure appears to be an oligopoly (Zhao et al. 2009). The

Table 1
Breakdown of the Spam Supply Chain

Stage	*Pharmacy*	*Software*	*Replicas*	*Total*
Unique URLs	346,993,046	3,071,828	15,330,404	365,395,278
Domains	54,220	7,252	7,530	69,002
Store-front styles	968	51	20	1,039
Merchants	30	5	10	45

Source: From a study of 45 merchants tracked by Levchenko et al. (2011).

Stone-Gross team infiltrated the Cutwail botnet and documented its offerings, which range from a bare bones rental of computation time on the compromised machines all the way to a user-friendly interface allowing a customer to create a mass mailing and test it against open-source spam filters before sending. Like publishers in the legitimate advertising market, botnets invest in significant fixed costs of ad serving, match advertisers with potential customers, and offer large reach.

To probe the demand side of the spam market, Levchenko et al. (2011), a team of 14 coauthors based at the University of California at San Diego and the University of California at Berkeley, developed spam feeds to identify examples of spam, a web crawler to follow advertised URLs, and botnet infiltration and botnet detection algorithms (see also John, Moschuk, Gribble, and Krishnamurthy 2009) to monitor botnet activity. Table 1 presents statistics on the merchants tracked through this technique. The first row shows that spam for only 45 merchants included 365 million distinct URLs during the data collection period. The second row of the table shows that there are more than 5,000 times as many URLs as domain names used by spammers. For example, a spammer might register the domain pharma.com and then host thousands of identical pages with different URLs on the same domain: "pharma.com/buy123.html," "pharma.com/purchase01.html," and so on. There are also more than 1,000 domain names per merchant. A merchant may be represented by several affiliate spammers, each of whom might register multiple domains. Large, reputable registrars generally reject applications for spammy-sounding domain names, such as those containing "med" or "pharm" (Kanich et al. 2008), but hundreds of registrars are willing to look the other way (Levchenko et al. 2011). Row three gives the number of "store-front styles" that represent individual user interfaces, each with a distinct look and feel. When law enforcement tries to shut down illegal sales, they look for identical storefronts and try to take them down all at once, so store-front variation helps a merchant avoid complete shutdown. For each pharmaceutical merchant, there are approximately 30 distinct store fronts; this figure is much lower for software and replicas. The final row of the table shows the number of merchants anchoring the market. Despite the large numbers of domains, URLs, and store fronts, only 100 merchants had a measurable market share of spam activity, and fewer than ten merchants account for over 80 percent of the market (Levchenko et al. 2011; Kanich et al. 2011).

After tracking the merchants via the botnets, Levchenko et al. (2011) placed 120 orders for the advertised goods, spread across the 100 identified merchants. The affiliated spammer usually hosts the entire consumer storefront experience; that is, the spammer generally collects payment information and then hands the transaction to the merchant before credit card authorization. Payment processing services for these merchants are quite concentrated: a total of only 17 banks serve the 100 merchants, with just three banks (from Latvia, Azerbaijan, and St. Kitts and Nevis) processing the payments for more than 75 percent of the transactions. Postage stamps on the packages revealed the physical locations where the goods originated: nearly all the pharmaceuticals came from India, for example, while replica watches generally came from China.

Overall, while spammers have nearly free entry in registering domains and renting services from botnets, merchants appear to face more significant fixed costs, especially in obtaining payment processing services. Only a small number of banks appear willing to take the risk of associating with gray-market merchants. This may explain why a relatively small number of merchants supply most of the market for these spam-advertised goods.

Assessing the Externality

What are the costs of spam to users, and how does it compare with the return to spammers? A widely cited report from Ferris Research (2005) placed the worldwide cost of spam in 2005 at $50 billion; Ferris raised its estimate to $100 billion in 2007 and $130 billion in 2009 (Jennings 2009). However, the Ferris reports did not describe how they estimated such key parameters as the amount of time per worker spent deleting spam; indeed, one of the authors of that report indicated to us that their work was "not a scientific survey," but that it attempted to be a lower-bound estimate. Regarding the returns to spammers, the most common estimate of profits involves the phrase "millions of dollars a day," which in turn apparently originated in a widely cited IBM press release.[2] In this next section, we find these widely cited estimates of user costs and spammer profits are somewhat exaggerated, but of the right order of magnitude.

Measuring the Diffuse Costs of Spam

The negative externalities imposed by spam include wasted time for consumers: both wading through irrelevant advertisements in one's inbox and missing an important message that went to the junk mail folder. They also include the costs

[2] See Malik (2008), "IBM Says Storm Worm Creators Making Millions Daily," ⟨http://gizmodo.com/354741/ibm-says-storm-worm-creators-making-millions-daily⟩. Phishing for account information in order to steal money is a form of online crime representing less than 0.3 percent of all email traffic. Researchers at Microsoft found that conventional wisdom was an overestimate by 50 of the true profits to phishing (Herley and Florêncio 2009).

of server hardware, which requires more than five times as much capacity as would be required in the absence of spam, as well as the costs of spam prevention services provided by firms to reduce the burden on end users.

The chief challenge in totaling up the social cost is credibly estimating the number of hours lost by people dealing with spam. Estimating the amount of spam that beats spam filters is difficult—after all, if we knew it was spam, we would have filtered it. We choose to examine success rates of spam in influencing consumer behavior, and use these to infer how many spam messages must have gotten through. Here we rely on the work of Kanich et al. (2008), who observed that out of 347 million attempted mailings for an online pharmacy, about 83 million were accepted for delivery rather than bounced; our question is how many arrived in the inbox versus the spam box. The 83 million messages accepted for delivery resulted in 10,500 clicks by consumers; we can estimate the number of spam messages reaching the inbox with an educated guess about the clickthrough rate for spam campaigns. We know legitimate email marketing for medical products has a clickthrough rate of about 1.1 percent (Email Marketing Metrics Report, 2011), while untargeted display advertising on Yahoo! usually has clickthrough rates of 0.1 percent or less. The clickthrough rate for spam email should be lower than the former but higher than the latter, because spam targets consumers more indiscriminately than legitimate email marketing, while email that reaches the inbox attracts more attention than the average web graphical ad. Using a clickthrough rate of 0.25 percent for spam, we estimate that about 4,200,000 messages (10,500 clicks divided by 0.0025 clicks/message) reached inboxes, out of 347 million messages sent. That is, we estimate that only about 1.2 percent of sent spam messages actually reach user inboxes.

As a consistency check on this estimate, we look at spammers' costs and revenues. Given the free entry of spammers (as opposed to botnets or merchants), we should expect them to earn zero profits. Stone-Gross, Holz, Stringhini, and Vigna (2011) estimate that spammers pay around $30 per million unblocked message deliveries (or five million emails sent, 80 percent of which were blocked by blacklisting). Spammers appear to earn about $50 per purchase (Kanich et al. 2011), so to break even each spammer will have to generate 8.3 million email sends.[3] Knowing that spammers earn about one purchase per 375 clicks (Kanich et al. 2008) and assuming as before a clickthrough rate of 0.25 percent, we estimate that 150,000 emails must reach inboxes in order to generate one purchase. That gives us an estimate of 1.8 percent of attempted spams reaching user inboxes (0.15 million out of 8.3 million messages). This estimate is slightly higher than our original estimate, but in the same ballpark.

Given this figure, we can arrive at an estimate of the total user cost of spam. Ninety billion spam messages were sent each day worldwide in 2010 (Symantec 2010; MAAWG 2011); we just estimated that 1.2 percent of these 90 billion get through to the consumer. (These 2010 figures ignore the subsequent 30 percent decrease in global spam due to the Rustock botnet takedown described above, though anecdotal

[3] The Kanich group found 1 conversion per 12.3 million emails sent, which is in the right ballpark.

evidence suggests that other botnets have been growing to fill the void.) A large fraction of this spam targets the United States: more than 90 percent of this spam was in English (Symantec, 2010), and Kanich et al. (2008) observe nearly 100 times as much spam going to the United States as to any other country. Suppose, then, that the average value of a user's time is $25 per hour, and that each piece of spam takes an average of five seconds to deal with. (False positives in the spam box are more costly, but so rare that we ignore them in this estimate.) This brings the total worldwide end-user cost of spam to nearly $14 billion per year.

As to the costs of anti-spam technology and hardware, Jennings (2009) in a report published by Ferris Research estimated the costs at approximately $6.5 billion worldwide, based on surveys of firms purchasing anti-spam solutions. This seems roughly correct, given that the largest anti-spam service provider, Symantec, had $6.2 billion in annual revenues in 2011, although it is hard to know exactly how much of the revenue for this firm was due to spam as opposed to network security. Other firms providing anti-spam services to corporate clients include McAfee, Trend Micro, and Barracuda. Our total should also include the labor costs of the staff who install and maintain the anti-spam solutions, and the costs of additional server capacity required by spam email. We believe $6.5 billion is a reasonable estimate for the total, which represents approximately $30 per user for just over a billion users.[4]

If firms were not investing in anti-spam technology, end users would be receiving 100 times as much spam, which given our estimate of the current time loss due to spam, would put the total economic loss at over $1 trillion. However, without any spam filtering it is unlikely that email would be a popular means of communication, so while one cannot take this number literally, it does give a feel for the magnitude of user time savings resulting from private investment in anti-spam technology.

Taken together, the total costs of spam worldwide today appear to be approximately $20 billion, in round numbers. Our estimate is half that of the widely cited Ferris Research (2005) number, because we use a lower value of end-user time, we ignore help-desk support for users struggling with spam, and we use a lower estimate of the number of spams that reach user inboxes.

Measuring the Private Returns to Spam

Researchers have used three tactics to estimate the revenues of botnets and merchants: 1) monitor botnet activity and infiltrate spot markets for spam services, 2) hijack a botnet to estimate the number of purchases generated by a merchant through a spam campaign, and 3) estimate order volume through periodically placing one's own orders and examining the gaps in the sequential order ID numbers.

As an example of the first approach, Stone-Gross, Holz, Stringhini, and Vigna (2011) infiltrated the (then prolific) Cutwail botnet. They were able to monitor every advertising campaign run on the botnet, recording message volume, purpose, and associated merchants. Next, the team infiltrated a private web forum operated

[4] For reference, Yahoo! Mail incurs anti-spam costs of approximately $55 million per year for 500 million active email accounts, a cost of $0.10 per account per year.

Table 2
Cost of Spam Advertising Relative to Other Advertising Media
(cost per thousand impressions (CPM))

		Breakeven conversion with marginal profit = $50.00	
Advertising vector	*CPM*	*Percent*	*Per 100,000 deliveries*
Postal direct mail	$250–1,000	2–10%[a]	2000
Super Bowl advertising	$20	0.04%	40
Online display advertising	$1–5	0.002–0.006%	2
Retail spam	$0.10–0.50	0.001–.0002%	0.3
Botnet wholesale spam	$0.03	0.00006%	0.06
Botnet via webmail	$0.05[b]	0.0001%	0.1

Sources: For direct mail, U.S. Postal Service website, For Super Bowl advertising, ⟨http://money.cnn.com/2011/02/03/news/companies/super_bowl_ads?index.hrm⟩. For retail spam and botnet wholesale spam, Stone-Gross, Holz, Stringhini, Vigna (2011); for botnet via webmail, Motoyama, Levchenko, Kanich, McCoy, Voelker, and Savage (2010).
Notes: Cost per thousand impressions (CPM) is the standard unit of measurement in the advertising industry. For spam email, an impression will be a "successful connection"—an email that is not screened out by IP blacklisting and so lands in either the inbox or spam folder.
[a] Direct Marketing Association (2012) reports 2.2%.
[b] Assumes botnet rental is delivery method.

by the botnet masters as a market for spam services. The authors document two ways to publish spam through the Cutwail botnet. Retail spam services were offered at $100 to $500 per million emails in this market. "Wholesale" spam service involves separately acquiring email address lists and renting time on the botnet's spam-send infrastructure. A monthly rental, capable of pumping out 10 million unblocked messages per day, was priced at $10,000, or about $33 per million emails. A more premium wholesale spam product, sending all messages through webmail accounts (and therefore incurring the higher cost of having to break CAPTCHAs), cost about one-third more. The authors estimate that the Cutwail botnet earned $1.7–4.2 million in profit during the 14-month period of study.

In Table 2, we convert the cost estimates for spam from the first research technique (Stone-Gross, Holz, Stringhini, Vigna 2011; Motoyama, Levchenko, Kanich, McCoy, Voelker, and Savage 2010) to the standard unit used in the advertising industry: cost per thousand impressions (CPM). For spam email, an impression will be a "successful connection"—an email that is not screened out by IP blacklisting and so lands in either the inbox or spam folder. To put the figures in perspective, we also include estimates for the cost of sending consumers messages via direct mail, Super Bowl advertising, or legitimate online advertising. We next suppose the average transaction, or "conversion" in online-advertising parlance, to produce profits of $50. Given this assumption, Column 3 gives the conversion rate necessary to break even on each form of advertising. For legibility, Column 4 restates the breakeven conversion rates in units of conversions per 100,000 ads.

Direct mail is the most expensive form of advertising, due to printing and postage costs; this medium thus requires high breakeven conversion rates of at least 2 percent. For the case of $50 profit per sales, standard online display advertising can be profitable down to a conversion frequency of 2 per 100,000 ads, while "premium display" would require 10 per 100,000 ads. Retail spam is profitable down to 0.2 conversions per 100,000. Bulk spam through wholesale botnet rental is sustainable with a mere 0.06 conversions per 100,000 ads, or about 1 in 2,000,000. Clearly, spam can be orders of magnitude less effective than traditional forms of advertising and still remain profitable.

The second research technique, hijacking a botnet, appears in the influential 2008 "Spamalytics" paper (Kanich et al. 2008), in which the researchers co-opted a portion of the Storm botnet by modifying the software instructions given to a set of downstream zombie computers. The modified instructions replaced the link to the spammer's storefront with a link to their own replica storefront. Users could place an order at the replica storefront, but would then receive an error message. The researchers could thus measure how many conversions would have been generated by the spam emails with their modified instructions.

In total, the group modified 345 million pharmaceutical emails sent from botnet zombies. Three-quarters of these were blocked through blacklisting, and the remaining 82 million emails led to a scant 28 conversions, or about 1 in 3,000,000. This conversion rate is far lower than what could be profitable for a retail spam campaign. We suspect that the reason for this lack of success is that a large portion of this major spam campaign went to large email providers like Yahoo! and Gmail and failed to evade their spam filters. We hypothesize that small-scale spammers can beat spam filters more easily and can spend time crafting creatively targeted campaigns; meanwhile, large-scale bulk campaigns spray email like a firehose, but the vast majority of it is blocked by filters.

The same research group also introduced the third estimation technique: placing sequential orders and drawing inferences from order ID numbers (Kanich et al. 2011). They began by making multiple purchases only a few seconds apart. Ten merchants were determined to use simple ascending rules for order IDs; for these merchants, the researchers placed a series of orders spaced over a period of six weeks. The order IDs fully revealed the quantity of other orders placed in the intervening time periods. The researchers also learned that one spammer hosted the images for its storefronts on a server belonging to someone else, which the spammer had hijacked through malware. The researchers notified the server's owner, who in turn gave them permission to monitor requests for the relevant image URLs, which provided reliable data on average order size and the basket of goods purchased. Each of these ten large spam-oriented merchants earned between $500,000 and $1.5 million per month in revenue—of course, profits would be lower. The researchers project that, in total, spam-oriented merchants receive gross revenues of about $180–360 million dollars annually.

We can check this revenue estimate using estimates of the prices and quantities of spam emails sent. As noted earlier, Symantec (2010) estimates the volume of spam at 90 billion attempted connections per day, 80 percent of which are refused

due to blacklisting. Similarly, the Yahoo! Mail team told us that in October 2011, they received approximately 30 billion attempted connections per day, 80 percent of which were bounced, just under 10 percent of which went to the spam folder, and just over 10 percent of which went to a user's inbox. If the unblocked 20 percent of spam is priced at $50 per million ("premium bulk" rates), this would amount to $600,000 worth of spam being sent to Europe and North America each day—so perhaps $750,000 worldwide. This figure seems a bit high given our previous estimate of just under $1 million per day in revenues for the entire supply chain (which must also include the cost of goods sold), but it is of the right order of magnitude.

Overall, we feel comfortable with an estimate of total industry revenue for spam-advertised goods on the order of $300 million per year. One might, in principle, want to include consumer surplus in a calculation of the total benefits of spam. However, because consumers who wanted these goods would likely be able to find them via online searches in the absence of spam, we assume that the consumer benefits are less than the total revenues earned by the spam industry. Since we have estimated the revenues rather than the profits of the spam industry, and we know there are marginal costs to the goods sold, we will assume for convenience that the revenues represent approximately the total surplus generated by spam, including both producer and consumer surplus.

The "Externality Ratio" of Spam in Context

Spam to end users costs around $20 billion annually, compared with approximately $200 million in surplus generated by the spam to these same users. The ratio of the cost of this externality to society relative to the ratio of private benefits it generates is about 100:1.

To put this magnitude into context, Table 3 provides estimates for the externality ratios associated with 1) the air pollution from driving a vehicle, and 2) the (nonviolent) stealing of automobiles. For driving, we use a low value for the benefit accrued to a driver, a figure just above the operation cost per mile. In reality, people make many inframarginal trips, valued by the consumer well over the marginal cost. The cost estimate comes from Delucchi (1998), who does a nice job of accounting for the social cost of the various air pollutants emitted by an automobile; time congestion externalities are not measured so this estimate should be viewed as the cost of driving on an uncongested roadway. (Interested readers are directed to Parry, Walls, and Harrington 2007, who survey the literature more broadly, including the matter of congestion costs.) Delucchi's preferred estimate for the social cost per mile was $0.06; using this figure gives an externality ratio of about 0.1, three orders of magnitude less than the value we obtain for spam. By contrast, stealing automobiles has a much higher externality ratio, as demonstrated by Field (1993). The societal costs include uninsured losses to victims, insurance premiums, law enforcement patrol costs, and the cost of prosecuting and incarcerating offenders who are caught. Adding it all up, the costs imposed on society by auto thieves are a whopping 7 to 30 times the revenue extracted from the vehicle theft.

In certain ways, nonviolent auto theft turns out to be a fairly close analogue to spam. The costs of both auto theft and spam are high, and are distributed diffusely

Table 3
Extracted Revenue, Imposed Costs, and Externality Ratios

Activity	*Revenue/benefit*	*Cost*	*Externality ratio*
Driving automobiles	\$0.60 per mile	\$0.02–0.25 per mile[a]	0.03–0.41
Stealing automobiles	\$400–1200 million per year	\$8–12 billion per year	6.7–30.3
Email spam	\$160–360 million per year	\$14–18 billion per year[b]	39–112

Sources: The source for the first row is Delucchi (1997), for the second row, Field (1993). (The *FBI Uniform Crime Report* (2010) places the vehicle value extracted by criminals in the same range as Field 1993.) The final row is based on the authors' calculations.
[a] Air pollution costs.
[b] Cost to end users.

across the majority of the population (because insurance rates and law enforcement costs account for the bulk of the costs of auto theft, as in Field 1993). Relative to other types of crime with poor insurance coverage, both have particularly diffuse costs. Unlike most crime, spam has no specifically identifiable victim, no especially wronged persons inspiring law enforcement to vigorously bring spammers to justice. In fact, some of the "victims" of spam, those who voluntarily make purchases from illegal advertising, arguably exert large negative externalities on the rest of society. Accounting for how much spam actually reaches the inbox, we estimate that only about 1 in 25,000 people needs to succumb to the temptation to make a grey-market purchase to make it profitable for spammers to inundate everyone with advertisements at current levels. From an economic perspective, one could view a law enforcement system as providing disincentives to make such purchases.

While the externality ratio of spam is large, the cost comes in the form of attention and time, not disease and death as in the case of air pollutants. We are not aware of any estimates of the externality ratio of violent crime, but if we use \$10,000,000 as the value of a life and say that a victim of a violent crime has one chance in 1,000 of death, then the expected value of the loss of life would be \$10,000. For comparison, the gains to an armed robber may have greater utility than the losses to a victim because of differences in the marginal utility of income, but any plausible estimate of this social welfare gain from this typical armed robbery places the externality ratio far higher than our estimates for spam. Thus, there are examples of externality ratios higher than that of spam, though these tend to have their harm concentrated in a small number of people. Various forms of air pollution are similarly diffuse to spam, and may have much larger social costs than spam, but their externality ratios are much smaller.

Policy Proposals

Considerable effort has gone into anti-spam measures. We already discussed many of the private (and cooperative) technological solutions that have been

adopted by firms in an attempt to reduce the social cost of spam. Here we consider public policy proposals from the legal and economic perspectives.

Legal Interventions

American spam legislation began in earnest with the Telephone Consumer Protection Act (TCPA) of 1991, which, as a response to rising fax machine spam, required fax marketing to be opt-in.[5] The legislation also required phone telemarketers to offer an opt-out. In 2003, a consumer challenge to unsolicited email was unsuccessful; the Pennsylvania Superior Court ruled in *Aronson vs. Bright-Teeth Now* (2003 Pa. Super 187, 824 A.2d 320) that email transmission, without the tangible costs of paper and toner, was legally different from fax transmission. The TCPA did little to stop telemarketing, especially with the *Aronson* decision, because opting out on a firm-by-firm basis was difficult and time consuming. However, the National Do-Not-Call Registry adopted in 2003 allowed consumers to opt out of all telemarketing (with some exemptions for nonprofits and politicians) by filling out a single form.

The first national legislation directed at email spam was the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. The cumbersome title created the catchy acronym "CAN-SPAM." The law requires unsolicited email to have a valid return address, to offer a simple opt-out option, and to identify itself as advertising in the subject line. The CAN-SPAM Act does not appear to have markedly affected the illegal advertising market (Sipior, Ward, and Bonner 2004). One reason is that much of spamming activity was already illegal, including the sale of counterfeit goods infringing on trademarks and intellectual property rights, or pharmaceuticals that are illegal to dispense without a prescription in many jurisdictions (or even to ship across state lines to a consumer with a valid prescription). In addition, jurisdictional boundaries hamper spam prosecutions. A spammer may be based in Latvia, work for a merchant in Moscow, send spam to the United States from a botnet with zombie computers all over the world, and have the final goods shipped from India. Governments around the world have not been willing to strain diplomatic relations with other countries over spammers.

A different legal tactic has been proposed by Levchenko et al. (2011). Recall that they found a potential choke point for spammers: the small number of banks willing to process payment for the merchants. American authorities might seek penalties for U.S. banks who transact with spammers in places like Azerbaijan, Latvia, and St. Kitts & Nevis. Indeed, some of the basis for such legislation could come from the war on drugs, since a fair number of spam purchases are for controlled narcotic substances such as oxycodone.

Economic Policy Proposals

To correct problems created by a negative externality, the standard solution in the economist's toolkit is to levy a Pigouvian tax on the externality-causing activity.

[5] Some illegal fax spam continued. Horror stories from recipients are documented at ⟨http://www.junkfax.org/fax/stories/Kirsch.html⟩.

In the case of spam, the popular economic solution is to require a "postage stamp," costing perhaps a tenth of a cent, for delivery of an unsolicited email advertisement, and transfer that postage amount to the receiver to compensate them for their attention (for example, Kraut, Morris, Telang, Filer, Cronin, and Sunder 2002; and Bill Gates at the World Economic Forum in Davos, Switzerland, in January 2004 as reported in Jesdanun 2004). However, pricing all email in order to disincentivize the irrelevant material is highly inefficient: many legitimate and useful emails, such as flight reminders and nonprofit newsletters, might well cease to exist.

A related option would be to levy penalties on consumers who purchase goods from spammers, on the grounds that every purchase goes a long way toward increasing the profitability of spam to U.S. consumers. However, enforcing such a law would be quite difficult without severe restrictions on privacy—like giving government the ability to monitor purchase receipts sent to webmail clients.

Instead, economic authors generally prefer the a variant of the Pigouvian tax called "attention bonds" (Loder, Van Alstyne, and Walsh 2004). The idea is to have the sender of an email pay the receiver for attention. The sender sends a bond—–for example, say five cents–along with each email. When the recipient reads the mail, the recipient gets the sender's five cents deposited in a bank account (or the recipient can choose to accept the email without payment, returning the money to the sender). The recipient can also "whitelist" a sender to receive all of future emails from that sender, even those with zero posted bond price. This whitelisting option is designed to avoid penalizing useful automatic emails like newsletters and flight-change notifications: solicited (whitelisted) emails have a zero price, which is efficient given the near-zero cost of transmission, while unsolicited emails have a positive price designed to compensate recipients for the imposition on their attention. Any (non-whitelisted) messages without the required bond never reach the recipient's mailbox. Ideally, consumers would have the ability to set individual thresholds for the price of their attention; for example, a high-school student might be willing to look at any unsolicited email whose bond exceeded half a cent, while a busy lawyer might require at least $20. Internalizing the attention externality in this way would give advertisers incentives to make sure they were targeting their emails only to those consumers most likely to be interested in the advertised products, thus increasing economic efficiency.

While we admire the elegance of attention bonds, we wish to sound a note of caution. No method currently exists to link email accounts with payment mechanisms. Should adoption of the attention bond proposal eventually become feasible, how might spammers respond? With attention bonds, a cybercriminal could earn the size of the bond per email, say $0.05 (a figure often suggested, see for example Van Alstyne 2007), by hijacking a legitimate account and sending mail to his own account to collect the bond. Account hijacking is already a serious problem, and the incentives to hijack would increase by at least three orders of magnitude if one could steal $500 by sending 10,000 emails from a hijacked account. Of course, countermeasures could then be taken, but our point is that the attention bond system will surely produce attempts to exploit the new system for profit. By the time one takes into account the transactions costs of setting up an attention bond system, along

with a much heightened incentive to hijack accounts, the overall welfare effects of such a change are unclear to us.

There are two key inefficiencies at work with the sender-push property right of SMTP. This paper has thus far focused on the first: unsolicited email imposes an externality on user attention. The second is that spam has arguably created a stigma for legitimate email marketers, destroying potential surplus that could be created by legitimate players who would, in the absence of such stigma, offer some well-targeted emails to consumers who would mostly appreciate them. This inefficiency has presented an arbitrage opportunity for middlemen, including "daily deal" sites like Groupon and LivingSocial. A daily deal site collects email addresses via consumers opting in. If the deals turn out not to be of sufficiently high quality, consumers can easily opt out with a single action (which is much easier than opting out of unsolicited emails from hundreds of individual merchants). Merchants reach consumers through the transmission rights of the middleman, and pay a substantial fee to do so. As of this writing in mid 2012, Groupon's market valuation exceeds $5 billion and it has about $1.8 billion in annual revenue, which gives one an idea of the size of this second inefficiency. The other major daily deal site, LivingSocial, is a private company, so revenue figures are not available, but the company controls a comparable market share to Groupon. There are many other competitors in this space, ranging from big players such as Google, to local newspapers. We view $5 billion as a reasonable estimate of the daily deal market.

In contrast to the high-level market-design interventions that have been proposed, we feel the most promising economic interventions are those that raise the cost of doing business for the spammers by cutting into their margins and thus making many campaigns unprofitable. As mentioned, one fruitful avenue is to put legal pressure on domestic banks that process payments from foreign banks known to act on behalf of spam merchants. This could put downward pressure on conversion rates and with them, profits. Another proposal comes from our colleague Randall Lewis, who imagines "spamming the spammers" by identifying spam emails and placing fake orders on spam-advertised stores. This step would increase the merchants' costs dramatically, as they would find it much more difficult to fill orders, and their banks may raise their fees if they submit many invalid payment authorization requests. Of course, an unintended consequence is that from time to time a legitimate merchant will be inundated with bogus product orders.

Email-spam advertising has evolved over the past 15 years from a handful of independent spam kings to a well-organized, sophisticated market. The spam supply chain includes merchants at the top, affiliate spammers downstream, and a relatively concentrated market of botnets producing the majority of the spam emails. Nearly 40 trillion spam emails per year advertise a variety of products, including pharmaceuticals, gambling, counterfeit watches, gray-market job opportunities, pornography, software, and dating services. The costs of spam to consumers outweigh the social benefits by an enormous margin, on the order of 100:1. While we admire high-level economic proposals to introduce Pigouvian taxes on spam, our research on the cat-and-mouse games played by spammers leads us to be cautious about the possible

unintended consequences of these proposals. Instead, we advocate supplementing current technological anti-spam efforts with lower-level economic interventions at key choke points in the spam supply chain, such as legal intervention in payment processing, or even spam-the-spammers tactics. By raising spam merchants' operating costs, such countermeasures could cause many campaigns no longer to be profitable at the current marginal price of $20–50 per million emails. These proposals are no panacea, but could bring about a significant reduction in spam.

■ *Both of us completed this work while working at Yahoo! Research. We thank Yahoo! for giving us an unprecedented opportunity to pursue research with academic freedom and access to corporate data. We are grateful to our former Yahoo! colleagues Carlo Catajan, Raghav Jeyeraman, and Gareth Shue for taking time to help us understand the institutional details of this market. Anirban Dasgupta, Randall Lewis, Preston McAfee, Kunal Punera, Michael Schwarz, and Andy Skrzypacz provided helpful discussions. We thank JEP editors David Autor, John List, Chiang-Tai Hsieh, and especially managing editor Timothy Taylor, for advice and support in structuring and revising this paper.*

References

Almeida, Tiago A. Almeida, Gómez, José María, and Yamakami, Akebo. 2011. "Contributions to the Study of SMS Spam Filtering: New Collection and Results." In *Proceedings of the 11th ACM Symposium on Document Engineering,* pp. 259–62. New York, NY: ACM.

Androutsopoulos, Ion, John Koutsias, Koutsias V. Chandrinos, George Paliouras, and Constantine D. Spyropoulos. 2000. "An Evaluation of Naive Bayesian Anti-spam Filtering." arXiv preprint cs/0006013. http://arxiv.org/abs/cs.CL/0006013.

Caballero, Juan, Chris Grier, Christian Kreibich, and Vern Paxson. 2011. "Measuring *Pay-per-Install*: The Commoditization of Malware Distribution." In *Proceedings of the 20th USENIX Security Symposium.* http://static.usenix.org/events/sec11/tech/full_papers/Caballero.pdf.

Caballero, Juan, Pongsin Poosankam, Christian Kreibich, and Dawn Song. 2009. "Dispatcher: Enabling Active Botnet Infiltration Using Automatic Protocol Reverse-Engineering." In *Proceedings of the 16th ACM Conference on Computer and Communications Security,* pp. 621–34. New York, NY: ACM.

Castillo, Carlos, Debora Donato, Aristides Gionis, Vanessa Murdock, and Fabrizio Silvestri. 2007. "Know Your Neighbors: Web Spam Detection Using the Web Topology." In *SIGIR'07: Proceedings of the 30th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval,* pp. 423–30. New York, NY: ACM.

Caverlee, James, and Ling Liu. 2007. "Countering Web Spam with Credibility-based Link Analysis." In *Proceedings of the Twenty-Sixth Annual ACM Symposium on Principles of Distributed Computing,* pp. 157–66. New York, NY: ACM.

Cho, Chia Yuan, Juan Caballero, Chris Grier, Vern Paxson, and Dawn Song. 2010. "Insights from the Inside: A View of Botnet Management from Infiltration." In *Proceedings of the Third USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET'10).* http://www.icsi.berkeley.edu/pubs/networking/insightsfrom10.pdf.

Cohen, David. 2012. "Busted: Fake Facebook Friend Requests." *AllFacebook: The Unofficial Facebook Blog,* February 28. http://allfacebook.com/facebook-fake_b79558.

Cook, Duncan, Jacky Hartnett, Kevin Manderson, and Joel Scanlan. 2006. "Catching Spam before It Arrives: Domain Specific Dynamic Blacklists." In *ACSW Frontiers '06: Proceedings of the 2006 Australasian Workshops on Grid Computing and E-Research,* Volume 54, pp. 193–202. Darlinghurst, Australia: Australian Computer Society.

Delucchi, Mark A. 1998. *The Annualized Social Cost of Motor-Vehicle Use in the US, 1990–1991:*

Summary of Theory, Data, Methods, and Results. UCD-ITS-RR-96-3(1), Institute of Transportation Studies, University of California, Davis. http://www.fhwa.dot.gov/scalds/delucchi.pdf.

Direct Marketing Association. 2010 "Response Rate Trend Reports." *DMA White Paper.* Available at: http://www.the-dma.org/cgi/dispannouncements?article=1451.

Evans, David S. 2009. "The Online Advertising Industry: Economics, Evolution, and Privacy." *Journal of Economic Perspectives* 23(3): 37–60.

Everett-Church, Ray. 1999. "The Spam That Started It All." *Wired Magazine,* April 13. http://www.wired.com/politics/law/news/1999/04/19098.

FBI. 2010. *Uniform Crime Report: Crime in the United States, 2010: Motor Vehicle Theft.* http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/property-crime/mvtheftmain.pdf.

Ferris Research. 2005. "The Global Economic Cost of Spam." Report #409.

Field, Simon. 1993. "Crime Prevention and the Costs of Auto Theft: An Economic Analysis." *Crime Prevention Studies,* Volume 1, edited by Ronald V. Clarke, 69–91. Lynne Rienner Publishers.

Ghiossi, Caroline. 2010. "Explaining Facebook's Spam Prevention Systems." *The Facebook Blog,* June 29. https://blog.facebook.com/blog.php?post=403200567130.

Gómez Hidalgo, José María, Guillermo Cajigas Bringas, Enrique Puertas Sánz, and Francisco Carrero García. 2006. "Content Based SMS Spam Filtering." In *Proceedings of the 2006 ACM Symposium on Document Engineering,* pp. 107–114. New York, NY: ACM.

Goodman, Joshua, Gordon V. Cormack, and David Heckerman. 2007. "Spam and the Ongoing Battle for the Inbox." *Communications of the ACM* 50(2): 24–33.

Gross, Doug. 2011. "Again? Sony's Playstation Network Hit with Another Attack." *CNN Tech,* October 12. http://articles.cnn.com/2011-10-12/tech/tech_gaming-gadgets_sony-playstation-network-attack_1_lulzsec-passwords-sony-pictures?_s=PM:TECH.

Herley, Cormac, and Dinei Florêncio, D. 2009. "A Profitless Endeavor: Phishing as Tragedy of the Commons." In *NSPW'08: Proceedings of the New Security Paradigms Workshop,* pp. 59–70. ACM. http://www.nspw.org/papers/2008/nspw2008-herley.pdf.

Isacenkova, Jelena, and Davide Balzarotti. 2011. "Measurement and Evaluation of a Real World Deployment of a Challenge-Response Spam Filter." In *Proceedings of ACM ICM 2011,* http://conferences.sigcomm.org/imc/2011/docs/p413.pdf.

Jennings, Richi. "Cost of Spam is Flattening—Our 2009 Predictions. Ferris Research, http://email-museum.cm/2009/01/28/cost-of-spam-is-flattening-our-2009-predictions/.

Jesdanun, Anick. 2004. "Is Metered E-mail a Viable Anti-spam Tactic?" *USA Today,* March 5. http://www.usatoday.com/tech/news/techpolicy/2004-03-05-metering-email_x.htm.

John, John P., Alexander Moshchuk., Steven D. Gribble, and Arvind Krishnamurthy. 2009. "Studying Spamming Botnets Using Botlab." In *NSDI'09: Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation,* pp. 291–306. Berkeley, CA: USENIX Association.

Kanich, Chris, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, and Stefan Savage. 2008. "Spamalytics: An Empirical Analysis of Spam Marketing Conversion." In *Proceedings of the 15th ACM Conference on Computer and Communications Security.* ACM. http://www.icsi.berkeley.edu/pubs/networking/spamalytics.pdf.

Kanich, Chris, Nicholas Weaver, Damon McCoy, Tristan Halvorson, Christian Kreibich, Kirill Levchenko, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. 2011. "Show Me the Money: Characterizing Spam-advertised Revenue." In *Proceedings of the 20th USENIX Security Symposium.* http://static.usenix.org/events/sec11/tech/full_papers/Kanich.pdf.

Kotadia, Munir. 2004. "Porn Gets Spammers Past Hotmail, Yahoo Barriers." *CNET News,* May 6. http://news.cnet.com/2100-1023-5207290.html.

Krause, Beate, Christoph Schmitz, Andreas Hotho, and Gerd Stumme. 2008. "The Anti-social Tagger: Detecting Spam in Social Bookmarking Systems." In *AIRWeb'08: Proceedings of the 4th International Workshop on Adversarial Information Retrieval on the Web,* pp. 61–68. New York, NY: ACM.

Kraut, Robert E., James Morris, Rahul Telang, Darrin Filer, Matt Cronin, and Shyam Sunder. 2002. "Markets for Attention: Will Postage for Email Help?" In *CSCW '02 Proceedings of the 2002 ACM Conference on Computer Supported Cooperative Work,* pp. 206–215. New York, NY: ACM.

Levchenko, Kirill, et al. 2011. "Click Trajectories: End-to-End Analysis of the Spam Value Chain." *IEEE Symposium on Security and Privacy 2011,* pp. 431–46.

Loder, Thede, Marshall Van Alstyne, and Rick Wash. 2004. "An Economic Answer to Unsolicited Communication." In *EC '04 Proceedings of the 5th ACM Conference on Electronic Commerce,* pp. 40–50.

Mailer Mailer, LLC. 2011. "Email Marketing Metrics Report." Corporate White Paper. Available at: http://www.mailermailer.com/resources/metrics/2011/click-rates.rwp.

Malik, Haroon. 2008. "IBM Says Storm Worm Creators Making Millions Daily." *Gizmodo,*

February 10. http://gizmodo.com/354741/ibm-says-storm-worm-creators-making-millions-daily.

Messaging Anti-Abuse Working Group (MAAWG). 2011. *Email Metrics Program: The Network Operator's Perspective.* Report 14. http://www.maawg.org/sites/maawg/files/news/MAAWG_2010_Q3Q4_Metrics_Report_14.pdf.

Microsoft. 2011. "Battling the Rustock Threat." In *Microsoft Security Intelligence Report, Special Edition*. Microsoft Corporation.

Moore, Tyler, Richard Clayton, and Ross Anderson. 2009. "The Economics of Online Crime." *Journal of Economic Perspectives* 23(3): 3–20.

Motoyama, Marti, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey Voelker, and Stefan Savage. 2010. "Re: CAPTCHAs—Understanding CAPTCHA-solving Services in an Economic Context." In *Proceedings of the 19th USENIX Security Symposium,* Volume 10.

Moyer, Edward. 2011. "Breach Exposes Chase, Capital One, TiVo Customers." *CNET News*, April 2. http://news.cnet.com/8301-1009_3-20050068-83/breach-exposes-chase-capital-one-tivo-customers/.

Ntoulas, Alexandros, Marc Najork, Mark Manasse, and Dennis Fetterly. 2006. "Detecting Spam Web Pages through Content Analysis." In *WWW '06: Proceedings of the 15th International Conference on World Wide Web,* pp. 83–92. New York, NY: ACM.

Parry, Ian W. H., Margaret Walls, and Winston Harrington. 2007. "Automobile Externalities and Policies." *Journal of Economic Literature* 45(2): 373–99.

Ramachandran, Anirudh, Anirban Dasgupta, Nick Feamster, and Kilian Weinberger. 2011. "Spam or Ham? Characterizing and Detecting Fraudulent 'Not Spam' Reports in Web Mail Systems." In *Proceedings of ACM CEAS 2011: 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference.* ACM Digital Library.

Ramachandran, Anirudh, Nick Feamster, and Santosh Vempala. 2007. "Filtering Spam with Behavioral Blacklisting." In *CCS '07: Proceedings of the 14th ACM Conference on Computer and Communications Security,* pp. 342–51. ACM Digital Library.

Sahami, Mehran, Susan Dumais, David Heckerman, and Eric Horvitz. 1998. "A Bayesian Approach to Filtering Junk E-mail." In *Learning for Text Categorization: Papers from the 1998 Workshop,* vol. 62, pp. 98–105. Madison, Wisconsin: AAAI Press.

Samosseiko, Dimitry. 2009. "The Partnerka: What is It, and Why Should You Care?" In *VB2009: Proceedings of Virus Bulletin Conference.* http://www.sophos.com/security/technical-papers/samosseiko-vb2009-paper.pdf.

Sipior, Janice C., Burke T. Ward, and P. Gregory Bonner. 2004. "Should Spam Be on the Menu?" *Communications of the ACM* 47(6): 59–63.

Stone-Gross, Brett, Thorsten Holz, Gianluca Stringhini, and Giovanni Vigna. 2011. "The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-scale Spam Campaigns." Presented at *LEET'11: 4th USENIX Workshop on Large-Scale Exploits and Emergent Threats.* http://iseclab.org/papers/cutwail-LEET11.pdf.

Symantec. 2010. *Messagelabs Intelligence: 2010 Annual Security Report.*

Symantec. 2012. "Intelligence Report, May 2012." May, 2012. Available at: http://www.symanteccloud.com/globalthreats/overview/r_mli_reports.

Templeton, Brad. Undated. "The Origin of the Term 'Spam' to Mean Net Abuse." http://www.templetons.com/brad/spamterm.html.

Thonnard, Oliver, and Marc Dacier. 2011. "A Strategic Analysis of Spam Botnets Operations." In *CEAS '11: Proceedings of the 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference,* pp. 162–171. AMC Digital Library.

Tran, Hung, Thomas Hornbeck, Viet Ha-Thuc, James Cremer, and Padmini Srinivasan. 2011. "Spam Detection in Online Classified Advertisements." In *WebQuality '11: Proceedings of the 2011 Joint WICOW/AIRWeb Workshop on Web Quality,* pp. 35–41. AMC Digital Library.

Van Alstyne, Marshal. 2007. "Curing Spam: Rights, Signals & Screens." *Economists' Voice* 4(2).

Warren, Christina. 2011. "How to: Avoid and Prevent Facebook Spam." March 28. http://mashable.com/2011/03/28/facebook-spam-tips/.

Yardi, Sarita, Daniel Romero, Grant Schoenebeck, and danah boyd. 2009. "Detecting Spam in a Twitter Network." *First Monday* 15(1). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2793/2431.

Zdziarski, Jonathan A. 2005. *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification.* No Starch Press.

Zhao, Yao, Yinglian Xie, Fang Yu, Qifa Ke, Yuan Yu, Yan Chen, and Eliot Gillum. 2009. "Botgraph: Large Scale Spamming Botnet Detection." In *NSDI '09: Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation,* pp. 321–34. Berkeley, CA: USENIX Association.

Zhou, Dengyong, Christopher J. C. Burges, and Tao Tao. 2007. "Transductive Link Spam Detection." In *AIRWeb '07: Proceedings of the 3rd International Workshop on Adversarial Information Retrieval on the Web,* pp. 21–28. New York, NY: ACM.

This article has been cited by:

1. Hidetaka Taniguchi, Hiroshi Sato, Tomohiro Shirakawa. 2018. A machine learning model with human cognitive biases capable of learning from small and biased datasets. *Scientific Reports* **8**:1. . [Crossref]
2. Gopi Sanghani, Ketan Kotecha. 2018. Incremental Personalized E-mail Spam Filter using Novel TFDCR Feature Selection with Dynamic Feature Update. *Expert Systems with Applications* . [Crossref]
3. Bo Li, Yevgeniy Vorobeychik. 2018. Evasion-Robust Classification on Binary Domains. *ACM Transactions on Knowledge Discovery from Data* **20**:2, 1-32. [Crossref]
4. Nan Feng, Zhenjing Su, Dahui Li, Chundong Zheng, Minqiang Li. 2018. Effects of review spam in a firm-initiated virtual brand community: Evidence from smartphone customers. *Information & Management* . [Crossref]
5. Alex C. Kigerl. 2018. Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction?. *Trends in Organized Crime* **21**:1, 62-78. [Crossref]
6. R. S. van Wegberg, A. J. Klievink, M. J. G. van Eeten. 2017. Discerning Novel Value Chains in Financial Malware. *European Journal on Criminal Policy and Research* **23**:4, 575-594. [Crossref]
7. Marco Deseriis. 2017. Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society* **34**:4, 131-152. [Crossref]
8. Nasser Mohammed Al-Fannah. Making defeating CAPTCHAs harder for bots 775-782. [Crossref]
9. E. Vance Wilson, Soussan Djamasbi, Adrienne Hall-Phillips. 2017. Cognitive factors that lead people to comply with spam email. *Journal of Organizational Computing and Electronic Commerce* **27**:2, 118-134. [Crossref]
10. Amelia Rickard, Jeffrey Wagner, Jonathan Schull. 2017. Observations on the technology and economics of digital emissions. *Technology in Society* **48**, 28-32. [Crossref]
11. Mamoun Alazab, Roderic Broadhurst. An Analysis of the Nature of Spam as Cybercrime 251-266. [Crossref]
12. Shu He, Gene Moo Lee, Sukjin Han, Andrew B. Whinston. 2016. How would information disclosure influence organizations' outbound spam volume? Evidence from a field experiment. *Journal of Cybersecurity* **2**:1, 99-118. [Crossref]
13. Alex C. Kigerl. 2016. Deterring Spammers. *Criminal Justice Policy Review* **27**:8, 791-811. [Crossref]
14. Hartmut Egger, Josef Falkinger. 2016. Limited Consumer Attention in International Trade. *Review of International Economics* **24**:5, 1096-1128. [Crossref]
15. Alessandro Acquisti, Curtis Taylor, Liad Wagman. 2016. The Economics of Privacy. *Journal of Economic Literature* **54**:2, 442-492. [Abstract] [View PDF article] [PDF with links]
16. Ali Rodan, Hossam Faris, Ja'far Alqatawna. 2016. Optimizing Feedforward Neural Networks Using Biogeography Based Optimization for E-Mail Spam Identification. *International Journal of Communications, Network and System Sciences* **09**:01, 19-28. [Crossref]
17. Alex C. Kigerl. 2015. Evaluation of the CAN SPAM Act. *Social Science Computer Review* **33**:4, 440-458. [Crossref]
18. Mohammad Taha Khan, Xiang Huo, Zhou Li, Chris Kanich. Every Second Counts: Quantifying the Negative Externalities of Cybercrime via Typosquatting 135-150. [Crossref]
19. Osvaldo Fonseca, Elverton Fazzion, Italo Cunha, Pedro Las-Casas, Dorgival Guedes, Wagner Meira, Cristine Hoepers, Klaus Steding-Jessen, Marcelo H.P.C. Chaves. A Spam Traffic Cost Analysis for Network Operators 41-49. [Crossref]

20. Bo Yang, Hechang Chen, Xuehua Zhao, Masato Naka, Jing Huang. 2015. On characterizing and computing the diversity of hyperlinks for anti-spamming page ranking. *Knowledge-Based Systems* **77**, 56-67. [Crossref]
21. Mitchell Hoffman, John Morgan. 2015. Who's naughty? Who's nice? Experiments on whether pro-social workers are selected out of cutthroat business environments. *Journal of Economic Behavior & Organization* **109**, 173-187. [Crossref]
22. Qian Tang, Andrew B. Whinston. Improving Internet Security through Mandatory Information Disclosure 4813-4823. [Crossref]
23. Mamoun Alazab, Roderic Broadhurst. The Role of Spam in Cybercrime: Data from the Australian Cybercrime Pilot Observatory 103-120. [Crossref]
24. Jafar Alqatawna, Hossam Faris, Khalid Jaradat, Malek Al-Zewairi, Omar Adwan. 2015. Improving Knowledge Based Spam Detection Methods: The Effect of Malicious Related Features in Imbalance Data Distribution. *International Journal of Communications, Network and System Sciences* **08**:05, 118-129. [Crossref]
25. Giovane Moura, Ramin Sadre, Aiko Pras. 2014. Bad neighborhoods on the internet. *IEEE Communications Magazine* **52**:7, 132-139. [Crossref]
26. Karlis Podins, Varis Teivans, Iveta Skujina. Low-cost active cyber defence 1-16. [Crossref]
27. Giovane C. M. Moura, Ramin Sadre, Aiko Pras. Taking on Internet Bad Neighborhoods 1-7. [Crossref]
28. Mamoun Alazab, Robert Layton, Roderic Broadhurst, Brigitte Bouhours. Malicious Spam Emails Developments and Authorship Attribution 58-68. [Crossref]
29. Ingo Vogelsang. 2013. The Endgame of Telecommunications Policy? A Survey. *Review of Economics* **64**:3. . [Crossref]