"Spam, Spam, Spam . . .": A CHAT Perspective

Md. Mijanur Rahman

This article is an attempt to make meaning of the genre of spam in e-mails from a writing researcher perspective. Using cultural-historical activity theory (CHAT) as a framework, the author uncovers some of the complexities of the genre of electronic troublemaking as a writing practice.

"Most of us using the Internet e-mail service," Guido Schryen observes, "face almost daily unwanted messages in our mailboxes. We have never asked for these e-mails, and often do not know the sender, and puzzle about where the sender got our e-mail address from" (1). The messages being talked about here are nothing other than "spam," which, according to Kevin Gao, is a kind of e-mail that is sent from an anonymous source to large numbers of people in an unsolicited manner (157). While most e-mail users may simply ignore spam as a genre of electronic troublemaking, from a writing researcher perspective, it is a literate activity that is worth looking into.

As it happens, spam e-mails take many different forms. While some spams work as product advertisements, some come with executable virus files, others surprise you with some get-rich-quick schemes like lottery winning notifications

[1]The term "spam" in lowercase referring to unsolicited e-mail, according to Costales and Flynt, is "attributed to a Monty Python skit in which a group of Vikings sang "Spam, Spam, Spam," increasing in power and volume until it eventually overpowered all other conversations" (6). "SPAM" in all uppercase is, however, a trademark of Hormel Foods Corporation, referring to a kind of canned meat substance (6). In this article, the term "spam" has, of course, been used in the sense of unsolicited e-mails that overpower the digital conversations.

and lucrative business proposals (Schryen 1). In this article, I am going to talk about only one example of the get-rich-quick category (i.e., spams containing lucrative, but easy-to-grab business proposals), in such a way that triggers answers to questions related to all types of spams in general. In so doing, I will be using cultural-historical activity theory (CHAT) with its associated terms of Production, Representation, Reception, Distribution, Activity, Socialization, and Ecology as an analytical framework to have a more robust understanding of the genre of spam than what a merely textual analysis can provide. This application of CHAT to spam revealed a whole new world to me.

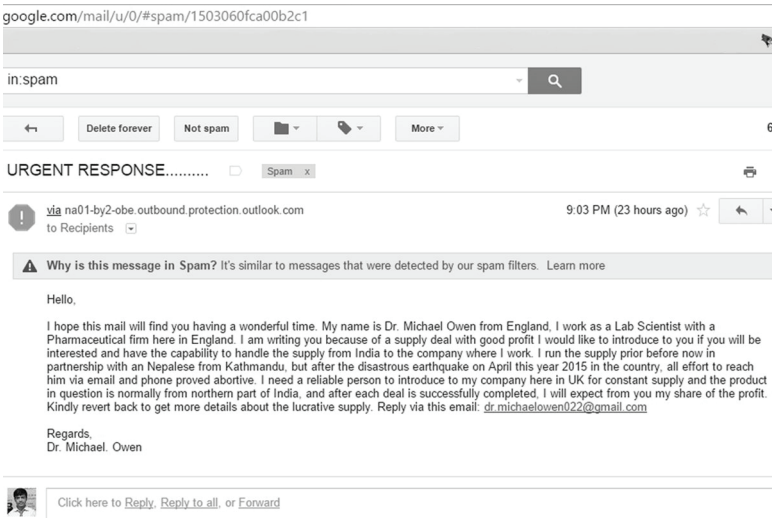

Figure 1: A screenshot of a randomly selected spam in my e-mail.

What does spam look like? In terms of appearance and textual features, it is like any kind of e-mail that we regularly exchange to communicate information and to do many other things (see Figure 1). But there is certainly something creepy about it that makes it spam. Just see who sent or produced this mail. If you always thought of the person signing in at the end of the e-mail as a producer of the e-mail, then one "Dr. Michael Owen" (who declares in the body of the e-mail that he is "from England" and works as "a Lab Scientist") would be considered the producer. But he is not. It is spam, after all. Have a look at the suggested reply e-mail "dr.michaelowen022@gmail.com." The guy reported to be "Owen" did not even use this e-mail to send the spam. If you look at the address at the top bar where you generally find the sender's e-mail address, it shows something like "via na01-by-2-obe.outbound.protection.outlook.com." Who in the real world would want to use this cumbersome e-mail address? These were things that made me more curious than ever.

In order to satisfy my increased curiosity, I kept asking a series of questions, such as "How does it get to my spam folder?" "Don't the

spammers target the inbox?" "What are the motivations behind troubling the e-mail users?" But answers to these questions, as you see, were not immediately identifiable just by looking at the body of the spam e-mail. This is where I turned to the framework of CHAT which, according to my understanding, allows us to see through the complexities of genres that we encounter in the world. In this genre research process, I also drew on a number of books on spam and e-mail marketing to produce a coherent and meaningful investigation here.

The first CHAT term I started investigating was the spam's **production**, which generally refers to "the processes and negotiations involved in creating texts under specific conditions, using specific tools, and following certain practices" (Sharp-Hoskins and Frost). The concept of tools, which overlaps with the concept of **distribution** (explained later), also seemed most interesting to me here. In terms of tools, the first thing that the spammers need is to gain access to our e-mail addresses. In a sense, spammers "harvest" people's e-mails from the web in a process that Jeremy Poteet calls "stealing candy from a baby" (4). People compromise their e-mail addresses in a number of ways making them vulnerable to spam abuse. They sometimes give away their own e-mail addresses themselves. "Obviously, if there was a large flashing neon sign saying SIGN UP FOR SPAM," Poteet explains, "few people would fill in the information" (7). But if there is a sign of a "giveaway" or a "deal," people often willingly sign up with almost any site. E-mail attackers are constantly looking for techniques like this to trick you into supplying your information. Be it a "cheap" health insurance quote or "a free vacation to a fancy location," we are very likely to give our "candy/e-mail" to the unsuspected spamming devils (7).

Our e-mail addresses get harvested not only from the forms we submit, but also from the websites that have our e-mails published. Spammers have numerous tools to extract e-mail addresses from these webpages. You may be surprised to hear that there is a type of computer program called *spambot*, a possible blended form of "spamming robots," that performs the e-mail harvesting by scanning any site that has your e-mails posted (Poteet 13). Forwarding groups of e-mails even in a friendly network can also expose them to spammers. Also, spammers or hackers can often guess many e-mail addresses by looking at the regularity of e-mail formation policy of any particular organization. As an example, can you guess how Illinois State University makes our e-mail IDs?[2] Hackers can also simply hack the web application to determine valid e-mail addresses (13).

[2]Illinois State University forms the first part of our e-mail addresses, also called ULID, by adding the first (and often the middle) initial followed by the first five letters of the user's last name, often adding a number to differentiate between people having similar initials and last name.

Apart from the tools aspect of production, the next CHAT term that bears a special relevance to spam is **distribution**, which is used to refer to "who a text is given to, for what purposes, using what kinds of distribution tools" (Sharp-Hoskins and Frost). According to Jeremy Poteet, "after a spammer has a list of e-mail addresses, their next step is to weed out invalid and inactive e-mails" simply by sending an e-mail to the address and seeing whether the message "bounces back" (39).

Besides checking the authenticity of the e-mails, the spammers try to find their right audience, too. The general rule, according to Poteet, is that they do not discriminate about whom they are sending the e-mails to while "selling sexual enhancement or the next get-rich-quick schemes" and they do it "*en masse*," though "many companies use services that target their mailings to particular demographic groups to maximize their returns" (9). You might be wondering, "How do they do that?" The question is tricky, but part of its answer lies in the fact that "when you provide your e-mail address, you're probably disclosing much more information that you realize" (9). They can also glean your Internet habits by simply locating your e-mail in different sites.

With the list of e-mails harvested, verified, and evaluated, the next step to spamming seems to be the easiest task ever, and the audience is apparently now just one click away from the spammers. But here comes the crux of the issue. What was supposed to be a simple press of the "send" button in e-mails turns out to be the most challenging job ever for the practitioners of the spam genre. The distribution of spam is not that easy as it is heavily impacted by two other scenarios which you can readily understand by using the CHAT terms activity and ecology. Then this intertwined concept of distribution, activity, and ecology forms a major point of focus in what is considered representation in CHAT. **Representation** refers to anything that happens before the production of a text, like the planning and designing of the spammers in furthering their aims in spamming. During this stage, the spammers need to consider elements surrounding the spam's activity and ecology very seriously. So, let us try to understand what these two terms mean as they relate to spam.

According to my understanding of Activity Theory, the AT of CHAT, the term **activity** is generally used to refer to a system in which multiple actors, human or non-human, with their own, often competing, goals make their own contribution to a social scene. The spammers do not live alone in a secluded world of digital technology. Their activity of sending spam en masse with their clandestine and dubious agenda is just one part of the **activity system** of e-mail service in the digital space, which is not only inhabited by the millions of vulnerable e-mail users but also by their service

providers and their stake-holding governments. These multiple actors play their own roles which can also be explained by another significant CHAT term, **ecology**, which "points to . . . the physical, biological forces that exist beyond the boundaries of any text we are producing" (Walker 161). Ecology presents two big hurdles for spammers: one is the laws of the stake-holding government, and the other is the filtering system of e-mail service providers.

The good thing is that the apparently unprotected inboxes of users like you and me do receive some legal protection by the State, which cares for how its citizens are inhabiting the electronic space, and whether this has any unwholesome impact on others. For example, the spammers do not always know the age range of the e-mail users who might be underage children. Spam containing adult content and services might do a serious disservice to them (Gao 158). Those who are not children also face possible risks in another way as spam is often designed to solicit sensitive and confidential financial information like "credit card details or personal data such as social security numbers that can be used for identity theft, credit card fraud, and a host of other crimes" (158). As part of their job to protect consumer rights, the Federal Trade Commission (FTC) enacted the CAN-SPAM Act of 2003. While this act is considered fairly ineffective at stopping spam from being sent to people's inboxes, the violators still run the risk of hefty fines if they get caught. This legal aspect of the spam's ecology, which, of course, exists beyond the boundary of e-mails in the actual physical world, always works as a limiting factor in spam distribution. That's why, in order to avoid the legal repercussions, the perpetrators often use a third-party server located outside the United States to send spam (158). This also explains why the spam from my inbox cited above has an odd-looking e-mail sender who people may not be able to track, or even if they are tracked, the law may not have enough jurisdiction to mete out justice to them.

So you might be thinking that the outside servers should effectively end the problem of distribution. But wait, the spammers have another ecological hurdle to cross, the biggest one in their attempt to sneak into the much-craved inboxes. The seemingly hapless e-mail users have another stakeholder to fall back on. In my case it is Google. E-mail service providers like Google have their own filtering systems in place that, in terms of activity, are in direct opposition to the activity system of spammers. The providers' care for the inbox is, however, a bit different from the way CAN-SPAM law cares. According to Gao, "for e-mail service providers, having a good spam filter is just good business" where the customer is a person with an e-mail account and their revenues are "based on the amount of time that a user spends in their inbox. Most of them, for example, serve web-based ads within the online version of an e-mail" (159). Keeping the user in the inbox increases

the likelihood that they will click on the online ads or at least see them more. Frequent spam could drastically reduce the frequency of the user's visits there, or they may even switch to other less distracting service providers (159). So providers like Google are commercially motivated in their activity of filtering and that must be overcome by the spammers to promote their competing interest in money-making.

What the above scenario indicates is that the distributors of spam need to take the spam filtering into account as it presents a sizable hurdle of ecology—diverting all unsolicited e-mails to the spam folder. The filter poses the trickiest challenge to the spammers as it works in accordance with an individualized algorithm that is not always accessible. However, a number of experts like Kevin Gao in his book on e-mail marketing and Vivian in the "Spam and suspicious e-mail" section of the *Google Support* website present a host of factors that work as stumbling blocks to spam. Their descriptions can be categorized into three major types of factors that help the filter identify spam as spam: content of the e-mail, action of the e-mail user, and network reputation.

In terms of content, any e-mail containing mature or adult content, explicit language, and get-rich-quick schemes (such as a lottery winning notification or a lucrative business proposal) will face the block (Gao 161–162; Vivian). The spam selected for close attention earlier in this article belongs to this get-rich-quick category. It offered me, and maybe millions of others, a chance to take up a supplier position that could tempt any commonsense business person, though it seemed too good to be true. To achieve this purpose of filtering based on content, the spam filter seems to have a built-in censoring dictionary containing words or lexical items that are typically associated with spam messages. Gao lists some 200 lexical items that could be flagged as spam. A few examples include "accept credit card," "big bucks," "cash bonus," "fantastic deal," "hidden assets," "Nigerian," "online biz opportunity," "Viagra," and so on (166–168). The second group of factors are the different types of actions taken by a particular e-mail user that might work as a filter. For instance, any e-mail that is blocked or reported as spam by users will end up being in the spam folder. Then, if the e-mails from a particular sender continue to remain unopened by the users, they may be flagged as spam. The final and third group of factors are the reputation of the senders and their domain names along with their presence in the international blacklist that decides whether e-mails from any source would be filtered as spams (Gao 161–162; Vivian). There is every possibility that the spam e-mail cited in this article was affected by this ecological constraint too, and the sender may not have been in the good book of Google as well.

Thus the spam e-mail as a genre on the fringe goes through a trajectory that is characterized by a number of activity systems working together with

competing and mutually contradictory objectives. But, you might wonder, why do spammers continue to send this troublemaking genre of writing to people? What is the use of it? How can they survive in their business? How many people are actually lured and why? Returning to CHAT, what is its reception? The answer is that there are a great number of people who have lost or exposed their candies/e-mails and are still vulnerable to deception. It may not be you or I as we are already in the know of things regarding spamming practices. But even if one out of a thousand or even a million responds to spam, compromising their confidential financial data, Gao argues, the purpose of the spammers is served so well that it may overshadow or outweigh the failures in millions of other cases (158).

I still remember the case of one of my younger brothers bringing me an electronic check, saying that he just needed credit card information to claim the $100,000 that he won on a random survey. Obviously, I made every attempt to make him understand the actual circumstances behind the hoax. However, he was not entirely pleased with my explanation because he, as part of the response to the spam, followed a set of distinct procedures to get the electronic check. My information saved him from the spam trick, but the world does not have a lack of people who are vulnerable to the traps of these get-rich-quick schemes. That said, "spam e-mail," according Gao, "is not an illogical business practice, it is simply an unethical one" (158). In terms of CHAT, spam e-mails have enough positive reception to make the business survive.

The distribution of spam features another dimension that has a lot to do with the way people receive spam in their individualized situations. It is, in light of the filters, now expected that the unsolicited e-mail messages will be diverted to the spam or junk folder in any given e-mail service, but there are two variations to this practice. One is that some spam still find its way into the inbox because spammers are smart people (often smarter than the Internet service providers) who continue to update their systems or practices at a faster speed than the providers do (especially the small organizations). An outdated filter cannot stop the spam. The second variation is just the other way around. This is reflected in what I have heard many of my friends saying: that some of their important e-mails end up being in spam folders. This situation is explained by a technical term in the world of e-mail service: "false positives" which refers to the "legitimate e-mail messages that are incorrectly marked as spam" (Poteet 151). While the filter can protect your inbox from "the unwanted e-mails," it runs the risk of sending your valid e-mail messages to the spam folders (2). This phenomenon helps to dissipate the binary of spam and regular e-mails, forcing many people to check their spam folder more frequently that they regularly do. The worrying factor is that false positives might occur when you are waiting for a job offer letter

because these e-mails contain many of the content features that a typical spam e-mail does as illustrated by the sample spam in this article.

Costales and Flynt, in their book on how to fight spam, visualize this situation as a kind of warfare between what they call "gorillas" and "guerrillas" (13). They note that "over the past few years spam e-mail has evolved from nuisance to scourge, now headlines speak of an antispam arms race and millions of dollars [being] lost in the battle with spams"(13). They observe that "the fight against spam has become a full-blown war" that is being fought "between the huge Internet Service Providers on the one hand (the gorilla) and the duck-and-run spammers on the other (the guerrillas), leaving most ordinary citizens in the role of a downtrodden populace" (13).

So what appears to be a simple cursory look at the spam (or even the inbox of e-mail) is actually a hotspot of a number of activity systems: the e-mail service provider attempting to block out the spam from the user's inbox, and the spammers doing everything in the world to sneak into people's seemingly unprotected inbox, all activities with a commercial purpose in mind dramatized on the hapless e-mail users. The unsolicited e-mail in your spam folder shows only a tiny fraction of what happens in the actual world as part of the complex and complicated digital practices which I might not have ever known if I hadn't used CHAT methodology in this research.

This study thus supports a much talked about point in writing studies that genres are a kind of "social action" (Miller 153). Spam is social action in that it is "typified rhetorical actions based in recurrent situations" of making money out of the digital space we occupy (159). Spam, as a genre, exists beyond the boundary of the text in a complicated social setting that needs to be taken into account if you want to understand it in its totality. Simply looking at the text could not help my understanding of spam, because spam (like all writing), is complex and complicated. Without the framework of CHAT, my writing research would have been seriously impaired here. So I end this article with the following unique mix of greeting and warning:

All Hail CHAT!!! Beware of Spam!!!

Works Cited

Costales, Bryan and Marcia Flynt. *Sendmail Milters: A Guide to Fighting Spam*. Addison Wesley Professional, 2005.

Gao, Kevin. *The Ultimate Guide to E-mail Marketing: Everything You Need to Know about Successful E-mail Marketing*. Comm100, emailmarketing.comm100.com/email-marketing-ebook/. Accessed 04 Oct. 2015.

Miller, Carolyn R. "Genre as Social Action." *Quarterly Journal of Speech*, vol.70, 1984, pp. 151–167.

Poteet, Jeremy. *Canning Spam: You've Got Mail (That You Don't Want)*. Sams Publishing, 2004.

Schryen, Guido. *Anti-Spam Measures: Analysis and Design*. Springer, 2007.

Sharp-Hoskins, Kellie and Erin A Frost. "Cultural Historical Activity Theory (CHAT)." *Isuwriting*, Spring 2012, isuwriting.files.wordpress.com/2012/07/chat_overview.pdf. Accessed 15 Nov. 2015.

Vivian. "Spam and suspicious e-mails." *Google*, 2015, support.google.com/mail/answer/1366858?hl=en. Accessed 4 Oct. 2015.

Walker, Joyce R. "Cultural-Historical Activity Theory: Because S*#t is Complicated." *Grassroots Writing Research Journal*, vol. 6, no. 2, Spring 2016, pp. 151–168.

Md. Mijanur Rahman is a second year PhD student in English focusing on TESOL/Applied Linguistics at Illinois State University. Pet dogs scare him; a sculpted tiger doesn't.