Spam as a Symptom of Electronic Communication Technologies that Ignore Social Requirements

Brian Whitworth
New Jersey Institute of Technology, USA

INTRODUCTION

Spam, undesired and usually unsolicited e-mail, has been a growing problem for some time. A 2003 Sunbelt Software poll found spam (or junk mail) has surpassed viruses as the number-one unwanted network intrusion (Townsend & Taphouse, 2003). *Time* magazine reports that for major e-mail providers, 40 to 70% of all incoming mail is deleted at the server (Taylor, 2003), and AOL reports that 80% of its inbound e-mail, 1.5 to 1.9 billion messages a day, is spam the company blocks. Spam is the e-mail consumer's number-one complaint (Davidson, 2003). Despite Internet service provider (ISP) filtering, up to 30% of in-box messages are spam. While each of us may only take seconds (or minutes) to deal with such mail, over billions of cases the losses are significant. A Ferris Research report estimates spam 2003 costs for U.S. companies at $10 billion (Bekker, 2003).

While improved filters send more spam to trash cans, ever more spam is sent, consuming an increasing proportion of network resources. Users shielded behind spam filters may notice little change, but the Internet transmitted-spam percentage has been steadily growing. It was 8% in 2001, grew from 20% to 40% in 6 months over 2002 to 2003, and continues to grow (Weiss, 2003). In May 2003, the amount of spam e-mail exceeded nonspam for the first time, that is, over 50% of transmitted e-mail is now spam (Vaughan-Nichols, 2003). Informal estimates for 2004 are over 60%, with some as high as 80%. In practical terms, an ISP needing one server for customers must buy another just for spam almost no one reads. This cost passes on to users in increased connection fees.

Pretransmission filtering could reduce this waste, but creates another problem: spam false positives, that is, valid e-mail filtered as spam. If you accidentally use spam words, like *enlarge*, your e-mail may be filtered. Currently, receivers can recover false rejects from their spam filter's quarantine area, but filtering before transmission means the message never arrives at all, so neither sender nor receiver knows there is an error. Imagine if the postal mail system shredded unwanted mail and lost mail in the process. People could lose confidence that the mail will get through. If a communication environment cannot be trusted, confidence in it can collapse.

Electronic communication systems sit on the horns of a dilemma. Reducing spam increases delivery failure rate, while guaranteeing delivery increases spam rates. Either way, by social failure of confidence or technical failure of capability, spam threatens the transmission system itself (Weinstein, 2003). As the percentage of transmitted spam increases, both problems increase. If spam were 99% of sent mail, a small false-positive percentage becomes a much higher percentage of valid e-mail that failed. The growing spam problem is recognized ambivalently by IT writers who espouse new Bayesian spam filters but note, "The problem with spam is that it is almost impossible to define" (Vaughan-Nichols, 2003, p. 142), or who advocate legal solutions but say none have worked so far. The technical community seems to be in a state of denial regarding spam. Despite some successes, transmitted spam is increasing. Moral outrage, spam blockers, spamming the spammers, black and white lists, and legal responses have slowed but not stopped it. Spam blockers, by hiding the problem from users, may be making it worse, as a Band-Aid covers but does not cure a systemic sore. Asking for a technical tool to stop spam may be asking the wrong question. If spam is a social problem, it may require a social solution, which in cyberspace means technical support for social requirements (Whitworth & Whitworth, 2004).

BACKGROUND

Why Spam Works

Spam arises from the online social situation technology creates. First, it costs no more to send a million e-mails than to send one. Second, "hits" are a percentage of transmissions, so the more spam sent means more sender profit. Hence, it pays individuals to spam. The logical goal of spam generators is to reach all users to maximize hits at no extra cost. Yet the system cannot sustain this. With 23 million businesses in America alone, if each sent just one unsolicited message a year to all users, that is over 63,000 e-mails per person per day. Spam seems the electronic equivalent of the "tragedy of the commons" (Hardin, 1968), where some farmers, each with some cows and land, live near a common grass area. The tragedy is that if the farmers calculate their benefits, they all graze the commons, which is destroyed from overuse. In this situation, individual temptation can undermine a public-good commons.

For spam, the public good is free online communication, and the commons is the wires, storage, and processors of the Internet. The individual temptation is to use the commons for personal gain. E-mail creates value by exchanging meaning between people. As spam increases, e-mail gives less meaning for more effort, that is, less value. Losses include wasted processing, storage, and lines; "ignore time" (time to reject spam); antispam software costs; time to resolve spam false positives; time to confirm spam challenges; important messages lost by spam; and unknown lost opportunity costs from messages not sent because spam raises the user cost to send a message (Reid, Malinek, Stott, & T., 1996). E-mail lowered this communication threshold, but spam makes communication harder by degrading the e-mail commons. If half of Internet traffic is spam, the Internet is half wasted, and for practical purposes, half destroyed. Spam seems to be an electronic tragedy of the commons.

SOME SPAM RESPONSES

If spam is a traditional social problem in electronic clothes, why not use traditional social responses?

Ignore It

One answer to spam is to ignore it: After all, if no one bought, spam would stop. However, a "handful of positive responses is enough to make a mailing pay off, and there will always be a handful of suckers out there" (Ivey, 1998, p. 15). There are always spam responders; a new one is born on the Internet every minute.

Ethics

Online society seems unlikely to make people more ethical than they are in physical society, so it seems unlikely spammers will "see the light" any time soon.

Barriers

Currently the most popular response to spam is spam filters, but spammers need only 100 takers per 10 million requests to earn a profit (Weiss, 2003), much less than a 0.01% hit rate. So even with 99.99% successful spam blockers, spam transmission will increase.

Revenge

One way users handled companies faxing annoying unsolicited messages was by "bombing" them with return faxes, shutting down their fax machines. For e-mail, ISPs, not senders, are registered. If we isolate ISPs that allow spam, this penalizes valid users as well as spammers. Lessig (1999) argued before the U.S. Supreme Court for a bounty on spammers, "like bounty hunters in the Old West" (Bazeley, 2003). However, the cyberspace "Wild West" is not inside America, nor under U.S. courts. And do we really want an online vigilante society?

Third-Party Guarantees

Another approach is for a trusted third party to validate all e-mail. The Tripoli method requires all e-mails to contain an encrypted guarantee from a third party that it is not spam (Weinstein, 2003). However, custodian methods require significant coordination and raise Juvenal's question, "Quis custodiet ipsos custodies [Who will watch our watchers]?" Will

stakeholders like the Direct Marketing Association or Microsoft guarantee against spam? If spam is in the eye of the beholder, such companies may consider their spam not spam at all.

Legal Responses

Why not just pass a law against spam? This approach may not work for several reasons (Whitworth & deMoor, 2003). First, virtual worlds work differently from the physical world. Applying laws online creates problems; for example, financial and health-care organizations by law must archive all communications so must not only receive spam, but also store it (Paulson, 2003). It is difficult to stretch physical law into cyberspace (Samuelson, 2003). Legal prosecutions require physical evidence, an accused, and a plaintiff, yet spam evidence is in a malleable cyberspace, e-mail sources are easily "spoofed" to hide the accused, and the plaintiff is everyone with an e-mail address. What penalties apply when each individual loses so little? Second, virtual worlds change faster than physical worlds. Spam can mutate in form, for example, Internet messaging spam or "spim." Any spam variant would require new laws, yet while society takes years to pass laws, the Internet can change monthly. Third, in cyberspace, code is law (Mitchell, 1995). Software can make spammers anonymous or generate new addresses so quickly that bans have no effect. Finally, laws are limited by jurisdiction; for example, state laws against telemarketers were ineffective against out-of-state calls, and the U.S. nationwide do-not-call list is ineffective against overseas calls. U.S. law applies to U.S. soil, but spam can come from any country. Traditional law seems too physically constrained, too slow, and too impotent to deal with the spam challenge. As Ken Korman (2003, p. 3) concedes, "Though legislative efforts to control spam continue, it is unlikely that new laws will have any real effect on the problem." *PC World* adds, "By all accounts, CAN-SPAM has failed to stop the e-mail inundation" (Spring, 2004).

Challenge Systems

Challenge systems, like MailBlocks (2003), ask e-mail senders, "Are you really a person? If so, type the number shown in this graphic." Since most spam is computer generated, and most spammers will not accept replies (lest they be spammed in return), such methods work well, but users communicate twice to receive once.

An E-Mail Charge

One way to change the communication environment is to charge for e-mail. This would hit spammer's pockets, but also reduce general usage by increasing the communication threshold (Kraut, Shyam, Morris, Telang, Filer, & Cronin, 2002). What would be the purpose of a charge, however small? An Internet toll would add no new service as e-mail already works without such charges. Its sole purpose would be to punish spammers by slowing the flow for everyone. A variant is that all senders compute a time-costly function (Dwork & Naor, 1993), but the effect is still to increase the transmission cost. Increasing across-the-board e-mail costs seems like burning down your house to prevent break-ins. If e-mail were metered, we would all pay for something already paid for. Who would receive each payment? If senders paid receivers, each e-mail would be a money transfer. The cost of administering such a system could outweigh its benefit, and who would set the charge rate? If e-mail providers took the charge, it would be an e-mail tax, but what global entity can legitimately claim it? Making the Internet a field of profit could open it to corruption. Spam works because e-mail costs so little, but that is also why the Internet works. Fast, easy, and free communication has benefited us all. To raise the communication threshold by charging for what we already have seems retrogressive. A solution that reduces spam but leaves the Internet advantage intact is to design for fair communication in the first place.

LEGITIMATE COMMUNICATION

Spam is an opportunity as well as a threat. The challenge is to close the social-technical gap (Ackerman, 2000) between society and technology. Traditional social methods, like the law, are struggling to do this. An alternative is for technol-

ogy to support society rather than being impartial to social needs. The Internet was once thought to be innately ungovernable, but it could just as easily become a system of perfect regulation and control (Lessig, 1999). If in cyberspace code, not law, makes the rules, it makes sense to design social software to support legitimate interaction, that is, social exchanges that are both fair to individuals and beneficial to the social group (Whitworth & Whitworth, 2004). This raises the question of whether spam is legitimate communication.

Is Spam Legitimate Communication?

Spam is unfair because senders have all the transmission choices, just like telemarketers who have your home phone number but invariably refuse to give you theirs. They call you at home, but you cannot call them at home. Spammers waste others' time, but this is irrelevant to them because it is not their loss. Yet the loss is still real, and it is unfair that those who cause it do not bear it, that those who suffer spam are not its creators.

Spam is unprofitable to society if its total losses exceed its total profit. If 90% of people spammed do not buy, do their losses balance the gains of the 10% who buy? What if 99.9% do not buy? There is a saturation point when spam's losses outweigh its benefits. We seem well past that point already. By one estimate, it costs about $250 to send a million e-mails, which cause about $2,800 in lost wages to society in general (Emery, 2003). Spammers steal time, which in today's world equates to money. Some see it as a mild crime, like littering on the Internet, but when litter blocks the streets, there is concern. Over millions of people the productivity loss is significant, as a cyber thief taking a few cents from millions of bank accounts can steal a sizable sum.

If spam is unfair to individuals and harmful to online society, it is illegitimate communication on two counts.

Communication Rights

The method of legitimacy analysis (Whitworth & deMoor, 2003) asks, Who owns the elements of e-mail communication: the messages, channels, and addresses?

Who Owns E-Mail Messages?

From a social-rights perspective, e-mail is a request, not a requirement, to receive a message. Receivers should be able to refuse ownership after reading it, perhaps via an e-mail toolbar rejection button. The receiver does not own a rejected message (by definition), and the transmission system does not own it, so it belongs to the sender who created it and, as with postal mail, should be returned to the sender. This does not happen because e-mail was designed as a forward-and-forget system, so replies to spammers may go nowhere (Cranor & LaMacchia, 1998), one reason the spam-the-spammer approach does not work (Held, 1998).

The social logic that communication is a two-way process implies that receiving back rejected e-mail should be a necessary condition of transmission. Rejected spam would then return down the sender's communication lines to their computer, creating spammer disk and channel costs. It seems inefficient to return rejected messages that can be deleted at delivery, but supporting social accountability in the long term both reduces waste and tells senders an e-mail was rejected. Currently, spammers do not know who reads their messages and who does not. If rejected e-mail were returned, it would pay spammers to reduce their lists and give them the information needed to do so. The right to reject e-mail is a social requirement. Implementing it is an engineering problem. The e-mail transmission system controls both the pieces of the communication game and the board itself. It should be able to enforce a rule that to send into the system, one must also receive from it.

Who Owns Communication Channels?

Current systems give any sender the automatic right to open a channel to another. Yet society gives no such "right to communicate," but rather the "right to be left alone" (Warren & Brandeis, 1890). The social concept is that one is not forced to communicate. To pursue undesired interaction is to harass or stalk. If someone knocks on our door, we need not answer. If they telephone, we need not pick up. But we get e-mail in our inbox, like it or not.

E-mail systems could present new messages in two parts: an initial "Can I talk to you?" channel

request, then the messages and content. Channel requests could give channel properties like the sender, title, and reciprocity (if replies are accepted; Rice, 1994), but not message content. Microsoft's plan to offer caller ID for e-mail seems a step in the right direction as it gives some channel information to receivers, but why not give all channel information? Receivers could then only receive messages from those who also receive. Current challenge-spam defenses offer this service but transmit content multiple times, and if the challenge bounces, they multiply spam.

Channel requests would send no content, only channel properties. The receiver can choose to open the channel or not. No third party need guarantee anything. No tedious challenges to sender humanity are needed. Sending messages is as before, except one could get a "channel unavailable" response. This is not a message rejection, but an unwillingness to talk at all. To receivers, messaging would also look the same, except unknown messages (like spam) would appear in a separate "Request to Converse" in-box, where users must double-click them to get content. Since most people do not click on spam, transmission volumes would reduce. Such handshaking occurs in data networks and could occur for e-mail. Giving known senders a permanent channel would create a self-generated list of known communicants (Hall, 1998).

Who Owns E-Mail Addresses?

The social concept of privacy suggests that people own their personal data. Good companies already include in their messages phrases such as, "To stop further e-mail, reply to this message." Yet these voluntary acts are not enough. Spammers can feign them, or worse, use your reply to confirm an active e-mail and sell your address to others. Requesting removal could put you on even more lists, becoming what *PC World* magazine calls "spam bait" (Spring, 2003): "By now, most computer users know that replying to most spam only generates more spam" (Woellert, 2003). Yet if users managed their own online data records, they could save companies data-maintenance costs.

FUTURE TRENDS

Currently, spam is tolerated by technology as the bandwidth can handle it. However, this may not continue. Some hope technology will continue to expand bandwidth and processing beyond the spam challenge, but simple arithmetic suggests otherwise. The spam potential increases as the square of the number of users, which grows each day. In a future with billions of people online, the potential interactions are beyond any technology we can presently conceive. The predictions are gloomy. Given current trends, it seems there is nothing to stop spam from becoming over 95% of Internet transmissions in a decade. Meanwhile, society's laws still struggle with telephone spam (telemarketing), let alone computer spam. The question seems to be not if e-mail will fail, but when.

Some experts suggest e-mail is already "broken," but will be replaced by new, and better, forms of communication (Boutin, 2004). Time will tell if this is true. If spam is a general social disease, it may cross application boundaries. Already, spim, a spam version of Internet instant messaging (Hamilton, 2004), is growing faster than spam ever did. Technology may not insulate us from antisocial acts in computer-mediated communication (CMC).

Spam seems to be a watershed moment, a critical point at which traditional social values and technology power confront. The stakes are high. If human society loses its way in cyberspace, the vision of an electronic global society may fade. A brighter scenario is that the legitimate-communication requirement will be recognized and technology redesigned accordingly; that is, the social-technical gap will close. Currently, the unity of global society is not political or legal, but technical. Society lets people return postal mail, but e-mail does not let people return messages. Society recognizes the right not to communicate, but e-mail gives a right to communicate. Society would let people remove themselves from marketing lists, but one cannot remove oneself from e-mail lists. Technology has the social requirements backward. Spammers force messages upon us that we should be able to reject. They access in-boxes we should own. They control e-mail addresses that should be ours. Technology gives

spammers every reason to do what they are doing, and no reason to stop.

If the social-technical gap were reduced, spam would also reduce. If e-mail could be returned to the sender and really arrive there, spam would reduce. If spammers had to "knock" before entering an in-box, spam would reduce. If e-mail users could remove themselves from e-mail lists, spam would reduce.

Such legitimacy-based changes have a unique property: They do not selectively discriminate spam or spammers. They would apply to all of us equally. Everyone's personal data would be their personal property. Anyone could converse or not. Any e-mail could be rejected, not just spam. The goal is legitimate interaction, not punishment or revenge, to reduce unwanted mail from all of us, not just spammers.

CONCLUSION

These conclusions can be summarized as follows.

1. Technology advances alone, like filters, will not in the long run reduce spam.
2. Traditional social solutions alone, like the law, will work poorly in cyberspace.
3. Spam is a social problem that requires a social solution.
4. The technical architecture of social-technical systems must support social requirements for social solutions to work.

The growing flood of spam from spam-generating to spam-filtering machines—information without meaning sent from no one to no one—seems a good place to start facing the social-technical challenge.

REFERENCES

Ackerman, M. S. (2000). The intellectual challenge of CSCW: The gap between social requirements and technical feasibility. *Human Computer Interaction, 15,* 179-203.

Albert, R., Jeong, H., & Barabassi, A. (1999). The diameter of the World Wide Web. *Nature, 401,* 130.

Bazeley, M. (2003, April 26). New weapon for spam: Bounty. *Mercury News.* Retrieved from http://www.siliconvalley.com/mld/siliconvalley/5725404.htm

Bekker, S. (2003, October 14). Spam to cost U.S. companies $10 billion in 2003. *ENTNews.*

Boutin, P. (2004, April 19). Can e-mail be saved? *Infoworld,* pp. 41-53.

Cranor, L. F., & LaMacchia, B. A. (1998). Spam! *Communications of the ACM, 41*(8), 74-83.

Davidson, P. (2003, April 17). Facing dip in subscribers, America Online steps up efforts to block spam. *USA Today,* p. 3B.

Dennis, A. R., & Valacich, J. S. (1999). Rethinking media richness: Towards a theory of media synchronicity. *Proceedings of the 32nd Hawaii International Conference on System Sciences,* HI.

Dodge & Kitchin. (2000). *Mapping cyberspace.* London: Routledge.

Dwork, C., & Naor, M. (Eds.). (1993). Pricing via processing or combating junk mail. In *Lecture notes in computer science: Vol. 74. Advances in cryptology: Crypto '92* (pp. 139-147). New York: SpringerVerlag.

Emery, T. (2003, January 27). Meeting takes aim at spam. *The Beacon Journal.*

Gibson, W. (1984). *Neuromancer.* London: HarperCollins.

Hall, R. J. (1998). How to avoid unwanted e-mail. *Communications of the ACM, 3*(41).

Hamilton, A. (2004). You've got spam! Spam not annoying enough? Now junk instant messages are on the rise. *Time,* pp. 1.

Hardin, G. (1968). The tragedy of the commons. *Science, 162,* 1243-1248.

Hauben, M. (1995). *The Net and netizens: The impact the Net has on people's lives* (Preface). Retrieved from http://www.cs.columbia.edu/~hauben/netbook/

Held, G. (1998). Spam the spammer. *International Journal of Network Management, 8*, 69-69.

Hiltz, S. R., & Turoff, M. (1985). Structuring computer-mediated communication systems to avoid information overload. *Communications of the ACM, 28*(7), 680-689.

Ivey, K. C. (1998). Spam: The plague of junk e-mail. *IEEE Computer Applications in Power, 11*(2), 15-16.

Korman, K. (2003). Canning spam. *netWorker, 7*(2), 3.

Kraut, R. E., Shyam, S., Morris, J., Telang, R., Filer, D., & Cronin, M. (2002). Markets for attention: Will postage for email help? *Proceedings of CSCW 02* (pp. 206-215).

Lessig, L. (1999). *Code and other laws of cyberspace.* New York: Basic Books.

MailBlocks. (2003). *MailBlocks is the ultimate spam-blocking email service.* Retrieved from http://about.mailblocks.com/

Mitchell, W. J. (1995). *City of bits space, place and the infobahn.* Cambridge, MA: MIT Press.

Paulson, L. D. (2003). Group considers drastic methods to stop spam. *Computer, 36*(7), 21-22.

Reid, F. J. M., Malinek, V., Stott, C. J. T. E., & T., J. S. B. (1996). The messaging threshold in computer-mediated communication. *Ergonomics, 39*(8), 1017-1037.

Rice, R. (1994). Network analysis and computer-mediated communication systems. In S. Wasserman & J. Galaskiewicz (Eds.), *Advances in social network analysis.* Newbury Park, CA: Sage.

Samuelson, P. (2003). Unsolicited communications as trespass. *Communications of the ACM, 46*(10), 15-20.

Spring, T. (2003, November 11). Spam slayer: Laws won't solve everything. *PC World*.

Spring, T. (2004, April). Spam wars rage. *PC World*, pp. 24-26.

Taylor, C. (2003, June 16). Spam's big bang. *Time*, pp. 50-53.

Townsend & Taphouse. (2003). *Spam is now number one source of unwanted network intrusions.* Retrieved from http://www.itsecurity.com/tecsnews/jul2003/jul141.htm

Vaughan-Nichols, S. J. (2003). Saving private e-mail. *IEEE Spectrum, 40*(8), 40-44.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.

Weinstein, L. (2003). Inside risks: Spam wars. *Communications of the ACM, 46*(8), 136.

Weiss, A. (2003). Ending spam's free ride. *netWorker, 7*(2), 18-24.

Whitworth, B., & deMoor, A. (2003). Legitimate by design: Towards trusted virtual community environments. *Behaviour & Information Technology, 22*(1), 31-51.

Whitworth, B., Gallupe, R. B., & McQueen, R. (2001). Generating agreement in computer-mediated groups. *Small Group Research, 32*(5), 625-665.

Whitworth, B., & Whitworth, E. (2004). Reducing spam by closing the social-technical gap. *IEEE Computer*, 38-45.

Woellert, L. (2003, August 11). Out, out damned spam. *Business Week*, pp. 54-56.

KEY TERMS

Asynchronous Communication: E-mail is normally considered asynchronous communication. Synchrony has been defined as "the extent to which individuals work together on the same activity at the same time" (Dennis & Valacich, 1999), but is e-mail synchronous if e-mail communicants are online at the same time? Another view is that synchrony requires instant transmission, but if e-mail became instantaneous, would it then be synchronous? Conversely, consider a telephone (synchronous) conversation during which one party boards a rocket to Mars; as the rocket leaves, there is a transmission delay of several minutes. Is the telephone now asynchronous communication? That the same medium is both synchronous and asynchronous is undesirable. Media properties should only change when

the medium changes; that is, they should be defined in media terms, not sender-receiver or transmission terms. The asynchronous-synchronous difference is whether the medium stores the message or not. In this, e-mail remains asynchronous no matter how fast it is, and telephone synchronous no matter how slow it is. The asynchrony is between receiver and medium, not receiver and sender. The opposite is ephemerality, in which signals must be processed on arrival.

Communication Environment: In one sense, technology operates in a physical environment, but for computer-mediated communication, technology is the environment, that is, that through which communication occurs. Telephone, CMC, and face to face (FTF) are all equally communication environments. FTF is mediated by the physical world just as CMC is mediated by technology. One cannot compare environments as one does objects in an environment. To judge one environment by another is like saying the problem with America is that it is not England. Describing e-mail as distributed rather than colocated is like this. If distributed e-mail correspondents magically colocate in the same room, what changes? In their environment, nothing changes at all. E-mail is not distributed or colocated because physical space does not exist in cyberspace. Nor do environments perform as objects do. Imagine a new environment called "underwater." Users find walking underwater painfully slow, then find a new way of moving (swimming) that fits the environment better, inventing flippers to support it. Now the new world seems better. Asking which environment is better at walking is inappropriate. Cross-media studies (CMC vs. FTF) make this mistake of analysing electronic communication in face-to-face terms (Hiltz & Turoff, 1985). A better approach is within-environment research designs (Whitworth, Gallupe, & McQueen, 2001).

Communication Threshold: The acceptable user cost to send a message (Reid et al., 1996). If the cost to send a message is less than the individual's messaging threshold, it is sent. Otherwise, it is not. E-mail lowered the messaging threshold so more messages were sent than otherwise would be.

Computer-Mediated Communication: CMC, like e-mail, is one-to-one, asynchronous communication mediated by electronic means. List e-mail seems to be many-to-many communication, but the transmission system simply duplicates one-to-one transmissions. In true one-to-many transmissions, like a bulletin board, one communication operation is transmitted to many people (e.g., posting a message).

Computer-Mediated Interaction: Computer-mediated interaction (CMI) is interaction mediated by electronic means, whether between people or computer agents.

Cyberspace: Space is central to our lives, whether virtual or physical (Dodge & Kitchin, 2001). Gibson (1984) coined the term cyberspace from the Greek kyber (to navigate), describing a nonphysical space (the "matrix") that substituted for reality. Today, it means the electronic environment that enables computer-mediated interaction. Cyberspace removes the physical space constraints of human interaction (Hauben, 1995) but is still a space, albeit of a different kind. Physical space locates us to a three-number coordinate position. Cyberspace also locates us to a unique URL (uniform resource locator) position. While physical locations have differing distances between them, points in cyberspace seem equally distant. If one moves through cyberspace by mouse clicks, cyberspace points could have distances between them. In theory, every cyberspace point is one click from every other, but in practice, this is not so. Research on the diameter of the World Wide Web suggests an average of 19 links between random points (Albert, Jeong, & Barabassi, 1999).

False Positive: A filtering system can make two types of errors: false acceptance and false rejection. The latter is a false positive. A spam filter can wrongly let spam through, or wrongly filter real e-mail as spam. In false acceptance, it is not doing its job, while in false positives, it is doing it too well. Decreasing one type of error tends to increase the other, as with Type I and Type II errors in experimental design. As the spam-filter catch rate rises above 99.99%, the number of false positives also rises.