You've Got Spam

By JONATHAN KOOMEY, MARSHALL VAN ALSTYNE and ERIK BRYNJOLFSSON

September 6, 2007; Page A16

In January 2004, Bill Gates boldly declared "two years from now, spam will be solved." Yet today, spam represents roughly 90% of all email sent. Spammers have thwarted both government and industry efforts to fix the problem, but a solution is within reach.

Unsolicited, unwanted, bulk email costs the global economy an estimated $50 billion each year in direct outlays, lost productivity, interruptions and wasted time. For all the wonders of the information age, it has also spawned a new form of "information pollution," where the actions of a few cost all of us dearly. The economics of the problem are simple: Incremental costs of sending an additional email message are nearly zero, so that even miniscule response rates make spam campaigns profitable. As communication costs drop further in coming years, the incentives for spammers to generate billions more emails will only grow.

Unfortunately, the anonymity of email inhibits traditional remedies for antisocial behavior, such as blocking out a prank caller's phone number or suing the sender of junk faxes. Most people cope by using spam filters, which identify and separate spam from legitimate email. This approach doesn't solve the problem -- because spammers can adapt as fast as filters can adjust -- but allows it to be managed.

The large email providers have experimented with different solutions to the problem but have been stymied by end-user resistance and territorial struggles over competing standards. There are two powerful approaches. One is "user authentication," where senders verifiably prove their identity so that "spoofing" is no longer possible (and spammers can be identified and shut down). The other is to use "sender bonds" that accompany email. As long as the value of the bond exceeds a prespecified hurdle (typically measured in pennies), the recipient will receive the email. After viewing the message, the recipient can then choose to claim the bond value or not -- seizing the bond makes the spammer pay for demanding attention, even if it's only the few seconds needed to delete a message. If even a small percentage of recipients claim the bond, spam campaigns will become uneconomic.

This past May, major email vendors settled on a standard for email user authentication called Domain Keys Identified Mail (DKIM), and some small email vendors now offer different types of sender bonds. Unfortunately, the larger

providers have not yet broadly adopted either solution, in part because of fears that some customers won't accept one or the other approach. Some users worry about privacy, and want to preserve email's anonymity (either to protect their own identities or the identities of important dissidents or whistleblowers). Others feel as a matter of principle that nobody should ever have to pay to send email.

The biggest obstacle, however, is the chicken-and-egg nature of the problem. Recipients can't insist on authentication or bonding because most email users don't have systems that support these solutions. Email providers don't offer these solutions because users aren't loudly demanding them. We're stuck at a bad equilibrium, even though a better equilibrium for everyone (except the spammers) is attainable.

To break this logjam, we advocate a hybrid system that would allow email users to *choose* their preferred email system. Those who want anonymity and no incremental cost for email can continue to send emails under the current system, without authentication and without sender bonds. Those who want the lowest costs and don't care about anonymity (most legitimate businesses would likely fall into this category) can send email that is user authenticated, but not bonded. People who want anonymity but are willing to pay to demonstrate the value they place on the recipient's attention can post a bond. Payment could be made anonymously via a clearinghouse, using the electronic equivalent of a tiny traveler's check bundled with each message. Those with especially high-value messages can make them both authenticated *and* bonded.

Email recipients would then choose which types of email they want to receive (as well as the monetary threshold at which they would accept bonded email). Our own choice would be to only receive email that is either authenticated or bonded (or both), and we suspect most others would quickly opt for this choice as well.

Achieving a hybrid system is feasible today, and implementing it is within the power of large email providers acting on their own, if they cease jockeying for private advantage and accept open standards. We have the technology. What remains is for us as users to stop accepting mediocrity. We will have a robust anti-spam infrastructure once we demand it from our email providers.

Mr. Koomey is a project scientist at Lawrence Berkeley National Laboratory and a consulting professor in the Department of Civil and Environmental Engineering at Stanford University. Mr. Van Alstyne is associate professor at Boston University. Mr. Brynjolfsson is professor at MIT's Sloan School of Management.