TACKLING SOCIAL CHALLENGES

I always find the The Profession column interesting, but February’s essay (Neville Holmes, “The Profession and the Big Picture,” pp. 104, 102-103) was particularly thought-provoking.

Indeed, it can hardly be said that “an effective percentage of the public can understand the relevant scientific evidence and reasoning.” However, by definition, democracy is power to the masses, and the average of any population is not going to be representative of the current peak of human knowledge in any field, scientific or otherwise.

Given the complexity of sustaining an enormous number of human beings on this planet with diminishing resources, it should be doubted whether democratic forms of government are intellectually capable of taking the complex and difficult decisions required. However, in Western developed countries, we currently seem to be living in an age where democracy is the end all and be all, the panacea that will solve all problems, and, above all, the one and only great truth that cannot be questioned.

New forms of representation and government should be envisioned, otherwise important decisions will be based on media spin and marketing criteria, rather than scientific principles.

Andrew Bertallot
Bernardston, Mass.
frengit@ieee.org

VOTING SYSTEMS

The ideas that Thomas K. Johnson puts forward in “An Open-Secret Voting System” (The Profession, Mar. 2005, pp. 100, 98-99) are basically sound. Indeed, the combination of computer-based entry and machine-readable paper ballot is ideal.

One aspect of this proposal, however, goes overboard, paving the way to totalitarian regimes that a democratic system is supposed to eliminate in the first place. Indeed, offering a way to return a ballot to the voter also introduces the possibility that organized groups could control the voting process by simply coercing citizens to give their voter ID when they exit the polls.

This has nothing to do with the technology in use: If there is any way to get an untampered voting receipt, a coercing organization could control the votes of its clients by requiring them to give this receipt to the organization. Then, it could verify without impunity how they voted.

This is the foremost reason why secret-ballot voting has been established in all democratic countries: Once a ballot is cast, there is almost no way to discover how a given person voted, other than asking him or her. I use the term “almost” because some inference can be made in local elections with a large enough number of candidates based on statistical patterns among a selected group of voters.

Therefore, the idea of assigning a unique voter ID must be proscribed from this scheme: There must be no way of tracing a ballot to a given voter, lest democracy vanish.

Didier H. Besset
Switzerland
didier@ieee.org

The author responds:
Consider this: There is no practical way to force anyone to vote in his best interests as opposed to giving in to pressure from those who might wish to gain votes through bribes or intimidation. The possibility that a citizen might sell his vote for money has always been with us. There already are ways to produce a copy of a ballot by using small cameras.

Obtaining votes through bribes or threats must be done one vote at a time, as “retail” vote theft. Ballot-box stuff- ing, tampering with voting machinery, and so on allow “wholesale” vote theft. In my humble opinion, the benefits of using the “open-secret” system to prevent the wholesale theft of votes outweigh the potential problem of their retail theft, at least in the jurisdictions I am most familiar with—the midwestern United States.

Perhaps in other parts of the world, the problems with voter intimidation might be too great to allow using printed receipts. But it occurs to me that there is another way to avoid the problem. If a voter chooses not to keep a copy of his ballot but wants to keep track of his ballot ID number, he could use a cell phone to transmit the number to a trusted friend or relative. Or he could use his phone to send the number via e-mail to his private e-mail address. He could then leave the polling place without having any record of his vote on his person.

As I stated in the conclusion to this article, I hope that a discussion of the benefits and problems with my proposal might lead to something even better.

The otherwise excellent “An Open-Secret Voting System” was marred by its fourth paragraph, which was a purely political statement that contributed nothing to the thesis of the article.

This paragraph suggests that the US should place a higher priority on fixing its own voting systems than on exporting democracy to other nations. The implications of this suggestion are astounding.

It means that, in the author’s judgment, it would be better for the Taliban to continue to oppress the people of Afghanistan, especially its women and girls, than to risk an attempt at democracy with less-than-perfect voting systems. It means that it would be better for hundreds of thousands of Iraqi citizens to be tortured or simply “disappeared” than to run the risk of a less-than-perfect vote tally in a peace-
ful, democratic transition of power.

Before this year, there was no risk that votes would be miscounted in Afghanistan and Iraq. There was also no risk that women in Afghanistan would enjoy the freedom to be educated or that Shiites in Iraq would enjoy freedom of religion.

Now, we do run the risk of vote miscounting. However, who could seriously suggest that living with this risk is worse than living under the prior governments?

I would like to make my own suggestion for an improved voting system: After each voter casts a vote, one of the voter’s fingers is marked with indelible ink to prevent fraudulent multiple voting. It’s not very high tech, but it has already been proven to work in two countries.

Ted Hills
Lambertville, N.J.
thills@comcast.net

The author responds:

Voting systems and democracy are political subjects by nature. It should not surprise any reader that an essay on the topic might include political statements.

Hills’s comments about the people of Afghanistan, oppression of women and girls, no risk of miscounting Iraqi votes, and so forth ignore some relevant facts: After the Iraqi military was defeated in the first Gulf War, the first Bush administration encouraged an uprising of Shiites against Hussein’s government. Then, as the Iraqi government used its remaining forces (including helicopter gunships) to slaughter the rebels, the US stood by and did nothing to stop the bloodshed.

Protection of the Shiites’ religious freedom, to say nothing of their very survival, was apparently not politically expedient at that time. But years later, after no weapons of mass destruction were found in Iraq, the second Bush administration decided that the liberation of the Iraqi people was a top priority, or at least, the reason du jour for “regime change.”

The suggestion about marking voters’ fingers with indelible ink may be workable in some settings. However, if there is a group that is intent on deterring voters from showing up at the polls (for example, Iraqi insurgents) the stained thumb could be hazardous to a voter’s health. The inked digit might be quickly amputated along with the offending hand or arm.

SOLVING THE SPAM PROBLEM

In his April column (The Profession, “In Defense of Spam,” Apr. 2005, pp. 88, 86-87), Neville Holmes offers an uncommon perspective with regard to spam. I think more people should adopt his view that “Technical solutions are always imperfect—at least to some degree. This provides a compelling reason to improve the technology, not to resort to legislation.”

I used that perspective to develop a technology solution for resolving the spam problem. In general, the current solutions can be described as filtering out spam. My concept is based on filtering in real-e-mail.

It is impossible to determine if an e-mail message is spam after it is sent. Instead, the solution—e-mail sender verification—is to provide a simple, easy to deploy way to verify real e-mails with embedded tags before sending them. The technology needed for verification is much simpler than authentication. Tampering with the tags can easily be detected, providing a simple means of differentiating between spam and real e-mail messages on the receiver side. The tag itself can be tampered, but the tampering is easily detected.

This solution will be 100 percent effective if both the sender and the recipient use it. Additional details are available at http://strategygroup.net/evs/.

Another issue encourages continuation of the spam problem: In some cases, adoption of a real solution for spam conflicts with business priorities. Any simple and effective solution to the spam problem would decrease the revenues of companies that sell anti-spam software, driving some into bankruptcy and leaving their consultants jobless. For more information on the strong efforts to keep this market growing, see “Filling the Gap Between Authentication and Spam Protection” by Hadmut Danische at http://www.ftc.gov/bcp/workshops/e-authentication/presentations/11-10-04_danisch.pdf.

George Mattathil
San Bruno, Calif.
george@StrategyGroup.net

Neville Holmes is a brave man to take a rational approach to spam. I hope his comments don’t generate too many irate letters from people who always think a new law will solve their problems.

My company and its competitors believe they have a solution to spam, albeit one that some SMTP hold-outs have yet to accept. Verizon has been sued for lost messages, so contract and constitutional laws may preclude ISP filtering as a solution.

Unlike SMTP, newer technologies can send XML messages securely using encryption for both storage and transmission. All senders are authenticated, and users can’t forge message headers. Each message has tracking, archiving, auditing, message retention, and electronic signatures built-in. Because it’s a “closed network that’s open to all,” a problem user can be restricted from sending through the network. It uses a federated architecture like regular e-mail, though each node is authenticated as well, so rogues can’t just set up a cheap server and hope to join the network. Marketing messages are
allowed because that’s the way the business world works, but spamming is definitely prohibited, and when uncovered, such senders can be cut off immediately.

Converting SMTP to something more secure and reliable will take time, just as e-mail itself took decades to grow. Businesses will drive the growth of better technologies more effectively than myriad, unenforceable laws. E-mail will become the CB radio of messaging, something left to the masses while businesses migrate to more trusted solutions.

David Wall
Kirkland, Wash.
david.wall@yozons.com

Neville Holmes responds:
I would like to think of it as adherence to professional principles rather than bravery. Anyway, living in Tasmania makes such bravery easy.

From the opening paragraph of “In Defense of Spam,” I get the impression that Neville Holmes thinks that spam is not a serious problem, but I can assure him that it is.

At last check, my account was getting more than 2,000 spam messages an hour, and the spam was actually coming in faster than my e-mail program could delete it. Even if the individual messages are quite short, this still represents an incredible amount of traffic, and it puts a significant financial load on all the parties involved in getting it to me.

I formerly ran an antivirus company, and I can only assume that some hacker thinks I still do and is trying to mount a denial of service attack.

Fortunately, most of the spam is of the type “random address”@provider, so I had my host bounce anything that is not addressed to either “my name” or “enquiries.” This, together with a few simple rules, has reduced the spam to a manageable level.

I agree that attempts to ban spam are unlikely to succeed, but I also believe that there is a very simple commercial solution to the problem. Junk snail mail is a nuisance, but it is tolerable because the senders must pay for it, so they will only send it if there seems to be a reasonable probability of making a profit. On the other hand, because of a historical accident, spammers don’t have to pay to send their messages, so they can operate profitably even though their success rate is extraordinarily low.

If we modify the e-mail protocols so that the sender has to pay a small sum for every e-mail he sends, spam would soon be reduced to manageable levels. More details are available at http://www.corybas.com/misc.htm.

Roger Riordan
Director, Cybec Foundation
riordan@cybec.com.au

Neville Holmes responds:
It seems quite a few readers inferred that by defending spam I was denying that there was a problem. My viewpoint actually is that spammers are the real problem, that the spam symptom would best be solved by technical and commercial measures such as Roger Riordan suggests, and that the governments of the world should be concerned about why people want to deceive and rob other people. This last point will perhaps be made clearer by an essay that is available online at society.guardian.co.uk/Print/0,518463-105909,00.html.

Letters