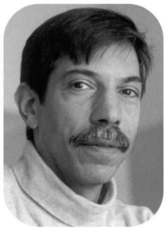
The Next Digital Divide



Fred B. Schneider
Associate Editor in Chief

A second digital divide is emerging. It threatens to promote irresponsible use of networked computing systems as well as to retard technological innovation through misplaced fears and ill-considered regulation. The sooner we eliminate this new digital divide, the better.

The first digital divide concerns computing—who has access and who doesn't. The second concerns understanding what is understood by technology users, developers, and regulators. Each of these communities has complementary and crucial roles to play in controlling the application and evolution of digital technology. Yet today, each has an incomplete picture of where things stand and where things are heading. So, addressing the second digital divide requires bridging multiple gaps in understanding.

Let's start with the user community. Today's users of computing services do not understand the extent to which they can trust software. Will some system perform as intended, despite the realities of mother nature, malicious attackers, and operator mistakes? Without understanding a computing system's trustworthiness, it is simply impossible to make good decisions about when and whether to depend on that system. Still, user communities go ahead with deployments. First, it is online student registration, then bank accounts or financial transactions, and, finally, national elections.

Our inability to measure system trustworthiness surely aggravates the problem. Nevertheless, existing knowledge in the technical community could better inform deployment decisions. So, part of addressing the second digital divide translates into an action item for those making deployment decisions: seek outside inputs from objective technologically knowledgeable sources. Of course, technologists must be willing to become involved when help is solicited.

Not all problems that originate with a technology will have solutions in that technology. Policies, legislation, and arbitration—in concert with tribunals or other courts having suitable jurisdiction—have a role to play. However, the technical community must be involved for these nontechnical solutions to be technologically sensible. For example, the current debate over computerized vote-tallying equipment illustrates this manifestation of the digital divide. The debate would have a different character absent the gap in understanding between those who seek to deploy this technology and those who study trustworthiness.

In contrast, the controversy regarding processor hardware extensions for trusted attestation and execution illustrates an apparent aversion by technologists to nontechnical solutions. A system in which security policies cannot be circumvented could give software producers and other content providers too much control over what can and cannot execute on a given computer—yet, a system in which security policies could be circumvented can hardly be called secure. Here, a regulatory solution could avoid what seems to be a Hobson's Choice, by limiting what policies third parties are allowed to impose.

Comfort in adopting regulatory solutions requires trusting that regulations can be written and enforced. Questions now arise about who has jurisdiction and who does the enforcement. But even ignoring these, recent experience with copyright protection legislation in the US (a single jurisdiction in which there is a culture of laws) does not bode well for placing trust that today's legislative bodies will produce sensible regulatory solutions for cybersecurity matters. Substantially greater involvement by disinterested technologists would undoubtedly have led to more sensible outcomes.

We might be able to spend our way out of the first digital divide; we're going to have to talk our way out of the second. All of us must spend more time interacting outside our respective communities. Participating in this dialogue will take time, and there is never enough of that, but without a dialogue, the regulations will come, and they will be ill-informed; the deployments will occur, and they will be overly conservative or recklessly optimistic; and the technological developments will continue, but they will be ignored or ineffective. □