From the Editors

**International Blues**

*IEEE Security & Privacy* could be a lot more international in its focus and content. Reflecting on its content and tone over the past seven years, it’s hard to tell that we think of either privacy or security in a broad international context. There are examples of taking a broader view, but they’re more notable as exceptions than as standards. This is bad for several reasons. First, privacy and security have different levels of importance in different places in the world. Second, by largely ignoring the non-Western world, we risk dangerous blind spots. Third, we might be failing to take simple steps that would make our magazine more valuable worldwide.

Although the purely technical aspects of our work are universal and generic, engineering is all about making trade-offs informed by economic and cultural judgments. Moreover, our subject matter firmly straddles the boundary between technology and policy—something we deliberately set out to do when we created the magazine in 2002/2003. Policy topics are generally more complex and tend to vary across jurisdictions, not to mention industries and institutions. Let’s begin to focus our attention on ensuring that our international relevance increases going forward.

We have seen far too few articles on the challenges of dealing with cybersecurity issues across jurisdictions. Definitions of criminal violations differ across the world—let’s see some examples of issues raised by these distinctions.

Cultural standards vary globally, leading to differences in attitudes toward security, privacy, and the role of security services. Maybe we can’t address generic technical questions yet, so perhaps we should be examining a range of case studies on how these subjects manifest themselves in different countries. After we’ve seen enough case studies, perhaps we’ll be able to abstract away from the details and get our heads around a new set of important questions. How have these variations affected security systems’ design and implementation and operational responses to incidents?

“Made in <insert country here>” has become meaningless as industries have globalized and the movement of physical and virtual goods has become ever easier, making accountability for product quality ever more diffuse—and assurance ever more difficult. Views of personal responsibility toward the community, the employer, the nation, and the world vary widely. An employer’s power to enforce behavior on the part of its employees varies widely across the world, so a vendor might well intend to deliver a high-integrity product, only to be undermined by one or more employees whose cultural views don’t require that they comply. One consequence of this is that products might have “features” that their operators never wanted, features that compromise the security and privacy guarantees that their operators seek to meet.

Can we begin a discussion of techniques for making networks robust in the face of components that are unreliable or even potentially hostile to our usage? Back in the 1980s, the MIT Project Athena folks argued that a security system’s design should presuppose that the network is held by hostile adversaries. Maybe it’s time to go back to that sort of design principle.

This topic isn’t brand new. For example, the United Nations Commission on International Trade Law has been working on cross-border computer crimes, trying to harmonize international agreements on things like rules of evidence, law enforcement cooperation, and definition of crimes. Numerous other international groups are now or can be expected to soon begin working on these and related issues. Cybersecurity is an area in which the balance of power between attackers and defenders is tipping very strongly toward the attackers. This situation presents challenges both to law enforcement and to national security institutions across the world, something that our community should begin to consider and address. *S&P* has been a leader in discourse throughout its life, and we will adapt ourselves to this emerging trend to best serve our community.

Marc Donner
Associate Editor in Chief