From the Reviews*

—-

What follows is a lightly edited selection of interesting, supportive, and contrary tidbits from the program committees reviews of the papers selected for HotNets V. The first, italicized paragraph summarizes the paper. The editing has conflated comments made by different program committee members, so I may refer to a melded PC hive mind rather than an individual. Of course, reviews reference the *submitted* versions of the accepted papers. The authors have addressed some, but not all, of our comments in their final copies; its interesting to see which comments led to revisions. We hope you enjoy this look behind the curtain.

NETWORK SYSTEM CHALLENGES IN SELECTIVE SHARING AND VERIFICATION FOR PERSONAL, SOCIAL, AND URBAN-SCALE SENSING APPLICATIONS

Articulates privacy and accuracy concerns that should be addressed by future applications that rely on sharing sensor data in personal, social and urban settings. A distinguishing feature of these applications is that the sensing devices, ranging from tiny motes to expensive video cameras, are owned and operated by individuals.

The application space the authors highlight is one that has been receiving plenty of attention, and deployment, in certain communities (HCI/ubiquitous computing, wireless), and were probably overdue for a networking paper on the topic. While the paper offers little new information, it does a nice job in pulling the discussion together and identifying the challenges, and could serve as a useful starting point for a discussion on the network implications of personal and urban computing.

While the straw-man architecture is useful, it's a bit of letdown in that it's mostly a formalization of how these applications are built today—i.e., a sensor network relays data to a server through a few proxies and clients query the server, again through a bunch of proxies. This proxy-centered architecture is traditional and somewhat limited; scenarios of a large number of mobile, autonomous, and yet related sensors (e.g., camera cellphones in the same city block, building) are at least as important and probably more challenging. Much of the novelty in your architecture seems to be in getting the selective sharing and context verification right, but it isnt clear how much of this is a networking issue, and the paper doesnt explore this in much depth other than telling us where in the infrastructure such functionality would be implemented. It would be nice to see a straw-man of data naming schemes, query language and pub-sub interfaces that might support some sample sharing and verification policies.

Are there organization/provider boundaries that need to be respected? Is this easily done with a DNS-like infrastructure that assumes an administrative hierarchy? What is the business relationship between client/sensors and their mediators, are there charging/accounting requirements? You say mediators are like firewalls in various ways, but if I am behind a firewall, I know who runs the firewall, and can hire and fire that person. I don't get the sense that mediators have that level of administrative "closeness" to their users.

"Citizen" is an odd word, but I have no alternative.

*This public review appeared in the HotNets V proceedings.