The Impending Debate

There’s some scary stuff going on in the US right now. President Bush says that he has the authority to order, without a warrant, eavesdropping on telephone calls and emails from and to people who have been identified as terrorists. The question of whether the president has this authority will be resolved by a vigorous debate among the government’s legislative, executive, and judicial branches, accompanied, if history is any guide, by copious quantities of impassioned rhetoric and perhaps even the rending of garments and tearing of hair. This is as it should be.

The president’s assertion is not very far, in some ways, from Google’s claims that although its Gmail product examines users’ email for the purpose of presenting to them targeted advertisements, user privacy isn’t violated because no natural person will examine your email. The ability of systems to mine vast troves of data for information has now arrived, but policy has necessarily lagged behind. The clobbering of Darpa’s Total Information Awareness initiative (now renamed Terrorism Information Awareness; http://searchsecurity.techtarget.com/sDefinition/0, sid14_gci874056,00.html) in 2004 was a lost opportunity to explore these topics in a policy debate, an opportunity we may now regain. Eavesdropping policy conceived in an era when leaf-node monitoring was the only thing possible isn’t necessarily the right one in this era of global terrorism. What the correct policy should be, however, requires deep thought and vigorous debate lest the law of unintended consequences take over.

Although our concerns in IEEE Security & Privacy are perhaps slightly less momentous, we are, by dint of our involvement with and expertise in the secure transmission and storage of information, particularly qualified to advise the participants in the political debate about the realities and the risks associated with specific assumptions such as what risks are presented by data mining. As individuals, we’ll be called on to inform and advise both the senior policymakers who will engage in this battle and our friends and neighbors who will watch it and worry about the outcome. It behooves us to do two things to prepare for this role. One, we should take the time now to inform ourselves of the technical facts, and two, we should analyze the architectural options and their implications.

Unlike classical law enforcement wiretapping technology (covered in depth in SEPPs November/December 2005 issue), which operates at the leaves of the communication interconnection tree, this surveillance involves operations at or close to the root. When monitoring information at the leaves, only information directed to the specific leaf node is subject to scrutiny. It’s difficult when monitoring at the root to see only communications involving specific players—monitoring at the root necessarily involves filtering out the communications not being monitored, something that involves looking at them. When examining a vast amount of irrelevant information, we haven’t yet demonstrated a clear ability to separate signal (terrorist communication, in this case) from noise (innocuous communication). By tracking down false leads, we waste expensive skilled labor, and might even taint innocent people with suspicion that could feed hysteria in some unfortunate future circumstance.

Who’s involved in the process of examining communications and what are the possible and likely outcomes of engaging in this activity? The security and privacy community has historically developed scenario analysis techniques in which we hypothesize several actors, both well- and ill-intentioned, and contemplate their actions toward one another as if they were playing a game. Assume your adversary makes his best possible move. Now assume you make your best possible response. And so on. In the case of examining communications at the root, we have at least four actors to consider.

One is the innocent communicator whom we’re trying to protect, another is the terrorist whom we’re trying to thwart. The third is the legitimate authority working to protect the innocent from the terrorist, and the fourth, whom we ignore at our peril, is the corrupted authority who, for some unknown reason, is tempted to abuse the information available to him to the detriment of the innocent. We could choose, in
recognition of the exigencies of a time of conflict, to reduce our vigilance toward the corrupted authority, but history has taught us that to ignore the concept puts us and our posterity in mortal peril.

Our community’s challenge in the coming debate is to participate effectively, for we occupy two roles at once. We are technical experts to whom participants turn for unbiased fact-based guidance and insight, and we are simultaneously concerned global citizens for whom this debate is meaningful and important. We must avoid the temptation to use our expertise to bias the debate, but we must also avoid being passive bystanders. We must engage thoughtfully and creatively. We owe this to our many countries, our colleagues, our neighbors, our friends, our families, and ourselves.

The views expressed herein are solely the views of the author and do not express the views of his employer. —Eds.