I start by recalling a simpler time, back when personal computing and networking were thought to be compatible. This may lead you to think that these paragraphs are a paean to the good old days and that therefore I am a naively nostalgic geezer. But they aren’t, and I’m not. Hear me out. Higher education has a tough choice ahead, and its origins lie back in a simpler time.

My first personal computer—let’s define “personal computer” as one that is not shared and that the user can equip and configure as he or she sees fit—was a two-floppy Rainbow, a short-lived Digital product with its own peculiar version of DOS. On my desk, the Rainbow joined a Lear Siegler ADM-3 smart terminal (“smart” then meant that remote hosts could move the cursor around on the terminal screen), which had a direct hard-wired serial connection to a Digital time-sharing computer, a PDP-11, if I recall correctly. Using my ADM-3 terminal, I could edit the contents of files on the PDP-11 and instruct that computer to compile, execute, or process them in various predetermined ways. The dominant use for my terminal was entering, editing, and analyzing statistical data. Until the Rainbow arrived, Labos used the terminal to enter text, to edit text, to compute, to print text, to process text, and to accept output from the Rain-}

bow and substituting a VisiCalc disk. I could do some limited data analysis and prepare well-formatted tables and graphs. My large raw statistical datasets and software remained on the PDP-11, accessible only through the ADM-3.

Early personal computing, for me and many others, thus comprised a few applications, but only one at a time; early networking comprised a single physical pathway from terminal to host. There was no conflict between the two. But two screens on one desk seemed silly, so I did physically removing disks to use different software: the time-shared PDP-11 had long before moved to shared storage and multiple applications running at a time. Soon personal computing and networking evolved. Inexpensive hard disk drives did away with physical application switching, terminal emulators did away with terminals like my ADM-3, and protocol-based networking did away with physically hard-wired networking. In today’s—the-better the reason software applications on personal computers came to communicate in myriad ways with all kinds of other computers and devices, rather than simply emulate a “terminal” talking to “hosts.”

The protocols for managing communication over shared networks became more complex, going beyond simple routing and transmission to manage competing demands on capacity and to accommodate creative new applications. Functionality and convenience expanded dramatically. Personal computing and shared networking had matured, in due course creating the networked personal computer, client-server computing, and the Internet. The marriage was a great success, a truly transformational innovation. Yet in retrospect, the seeds of today’s conflict were evident already at the goals for personal-computing progress were user flexibility, autonomy, and control, whereas the goal for networking work was automated management of a shared resource. One sought autonomy, the other authority.

Let’s return to the present. My mother, far from a technophile, uses a 2-GHz E Machines computer with a flat screen, a color printer, a DVD player, a CD burner, an Ethernet connector, and a built-in modem. The computer is set up just the way she likes it. She typically runs at least four applications simultaneously: her email and instant messaging, a word processor, a database, and a graphics viewer. She enjoys the kind of flexible multitasking that I could only dream about with the Rainbow. Since for the moment the only connection from my mother’s computer to the outside world is dial-up AOL, the network rarely in-}

trudes—even though through AOL she uses the Internet to read e-mail, to connect to very diverse services, but its price is compliance with network manage-}

ability on the shared network. Yet you cannot have network security if people have the capability and autonomy on the personal computer. The typical ISP limits security commit-}

ments to induce computing homogeneity and network security in that environment. But they have no choice but to run the typical college or university computer without virus protection or a host or firewall, for example, or to use a simple password, or to not keep application software updated, is to invite compromise by outsiders. Compromise, all but certain for the inattentive, guarantees that one’s computer will be removed from the network for attacking others; even vulnerability to compromise, if detected by my network-security staff, can lead to this result. The high-speed networking inter-}

connecting the University of Chicago community provides unprecedented access to very diverse services, but its price is compliance with network manage-}

ments to minimize constraints on its cus-}

tomers. The typical college or university does not. It thus finds itself spending exponentially more on network manage-}

ment, incident response, and small-scale disaster recovery. And the typical college or university CIO—someone like me—receives an increasingly vituparous array of how-dare-you-tell-me-what-to-do e-

mails and voice-mails. More problematic and expensive in the long run, the typical college or university finds itself using horribly complicated mechanisms to induce computing homogeneity and network security in its environment that violates the right of free choice and individual or de-}

partmental autonomy.

Obviously, this unmitigated conflict cannot continue. Equally obviously, given the legal and substantive risks, network security and therefore authority will trump auton-}

omy and personal computing. Colleges and universities will impose increasingly stringent requirements on network users, using both policy and tech-}

nology. The challenge, at this point, is rhetorical rather than technolog-}

ical. Colleges and universities will be able to dictate, and whether security requirements will constrain users—generally the focus to the question of how to find the right balance among rewards, punishments, and technology, how to frame the issues so that everyone understands them and come to consensus, how to maintain functionality in the face of re-}

striction, how to compare fixed and prob-}

abilistic estimates, and what to do if they maintain participatory governance when understanding options requires techno-

logical sophistication.

Gregory A. Jackson is Vice President and Chief Information Of-}

icer at the University of Chicago. He is the Viewpoints department editor for EDUCAUSE Review.

By Gregory A. Jackson

Network Security versus Personal Computing: Which Will Win?

Gregory A. Jackson