

# Whose Data Are These, Anyway?

A few years ago I had lunch with Ray Cornbill, a friend of mine who is a distinguished professor, though not a physician, at a major medical school. Ray's unique sideline is as an international rugby coach. We chatted about our work and compared notes on

current events. As we finished our lunch and prepared to depart, he made a remarkable statement: "I'm going over to the radiology practice to pick up my old x-rays."

What did he mean by that? It turns out that the radiology lab that had taken his x-rays for the past couple of decades decided that it could no longer afford to keep the old ones around. Because he was a well-known professor at an affiliated medical school, a staff member had given him the heads up about the imminent disposal. Why did he care? Well, before becoming a rugby coach, he was an active rugby player for many years. Rugby is, shall we say, a rather vigorous sport, and he had suffered several injuries to various parts of his musculoskeletal system. His x-rays represented his physical history; he felt strongly that losing this history would make it harder for his doctors to care for him in the future, so he wanted to collect them before they were discarded. Notice that he wasn't endangered by disclosure of confidential information, but rather by the loss of valuable historical data.

You go to a doctor or a hospital for an x-ray, but did you ever wonder who "owns" that x-ray? Your doctor ordered it and analyzed it, the radiologist made it and stored it, your insurance company paid for

it—but it's a picture of your body and is probably of the most value to you. But possession is nine-tenths of the law, as they say.

More than who has ownership claims, however, this question raises the issue of what ownership is. If we were to express the rights of ownership as methods in C++, they'd have names like these: Copy. Move. Destroy. Read. Modify. Transmit to someone else. The lab invoked its "ownership by possession" right in planning to destroy the x-rays. This is not entirely unfair; after all, the lab had spent money for years to store them and it is reasonable for them to want to stop spending money without a return. But in doing so it ran up against others' unarticulated but valid ownership claims.

Lately, much discussion in our community has focused on digital rights management (DRM), which seems mostly an examination of copyright law and how it might change in light of current technological advances. The debate has grown heated as the ability to use technology to recast the terms and conditions of, for example, the sale of a book or recording have penetrated the awareness of both sellers and buyers. As the likes of Lawrence Lessig of Creative Commons and

Clifford Lynch of the Coalition for Networked Information point out, the doctrine of first sale can be overthrown technologically. There might come a day when the fact that you've paid for a book doesn't mean that you can lend it to a friend or even reread it years later. This has huge implications for libraries and educational institutions, as well as for people who ever replace their computers or DVD players. These important issues are currently being debated in a wide range of fora.

What is most troubling, however, is that the only model that seems to get serious attention is wrapped around broadcast-like models of distribution—models with a few producers and many consumers, such as books, music, movies, cable TV, broadcast TV, and radio. Questions such as rights management for things like x-ray images and medical records in general don't attract much attention. For these sorts of intellectual property, we have to think more deeply about rights such as the right to destroy, the right to disclose, to publish or otherwise render unsecret, and others. Some work has been done in this area, such as for items like news photos, which tend to distinguish between the rights of celebrities and those of the rest of the population. The owners of important buildings have begun to assert rights to pictures that professional photographers take of them. And the performing arts community has established, by contract and practice, a system of fractional rights (primarily for managing royalty streams) that has some interesting characteristics.



MARC DONNER  
Associate  
Editor in Chief

Of course, this debate is not just about x-rays. It's about any of your information sitting in a folder in your doctor's office or that your bank has on file. Certainly the medical community, struggling with new HIPAA rules governing medical privacy, doesn't seem to have managed to provoke an engagement from the computer-science

and software-engineering research community. This is unfortunate for several reasons: our community has the ability to make a unique and valuable contribution to the discussion, and now is the time to resolve conceptual issues and design decisions so that the next generation of infrastructure can accommodate the emerging requirements. □

## S&P Board Member Receives Pioneer Award

The Electronic Frontier Foundation (EFF) held its 13th Annual Pioneer Awards on 22 April in Oakland, California during the 2004 Computers, Freedom & Privacy conference. The online civil liberties group honored Kim Alexander, David Dill, and Aviel Rubin for "spearheading and nurturing the popular movement for integrity and transparency in modern elections." The EFF ([www.eff.org](http://www.eff.org)) is a civil liberties organization that works to protect rights in the digital world.

Since 1991, EFF's Pioneer Awards have recognized individuals who have made significant and influential contributions to the development of computer-mediated communications or to the empowerment of individuals in using computers and the Internet.

Avi Rubin, computer science professor and technical director of the Information Security Institute at Johns Hopkins University and an *IEEE Security & Privacy* editorial board member, led the effort to expose security flaws in Diebold computer-based voting systems, combining technical skill and articulation to the public "in such a way that his solid technical work could not be ignored by those who would prefer an insecure status quo."

In 2003, Rubin coauthored a report that focused on Diebold and the integrity of electronic voting machines. He also coauthored an analysis of the US government's planned Serve system for Internet voting for military and overseas civilians, which ultimately led to that project's cancellation.



### INFORMATION ASSURANCE RESEARCH AND ENGINEERING

The Johns Hopkins University Applied Physics Laboratory (APL), a national leader in scientific research and development located midway between Baltimore and Washington, DC, is seeking qualified researchers and systems engineers to join APL's information assurance team.

#### Senior Information Assurance Researcher

Senior researchers who want to solve critical problems are needed to further the development of information assurance concepts and technologies. Join the APL team and apply your state-of-the-art knowledge to investigate methodologies for developing measurably secure components and systems. Enhance your leadership skills while working on interesting problems to secure critical network infrastructure and enhance national security. Propose and investigate new research concepts through internal research funding and external sponsorship. Qualifications include an MS or PhD in engineering, computer science, math or equivalent and 5+ years of related experience. Familiarity with networking concepts, information assurance technologies and techniques is essential. Familiarity with wireless protocols, modeling and simulation, and the demonstrated ability to lead projects are preferred.

#### Information Assurance Systems Engineer

Creative problem-solvers are needed to perform information assurance systems engineering for DoD's evolving network infrastructure. Join a newly forming engineering team in the rapidly expanding field of information assurance. You will participate in architecting the information security of systems central in DoD's transformation to network-centric warfare, including Global Information Grid (GiG), systems such as GIG-BE, Teleport, NCES, WIN-T and FORCEnet. Your responsibilities will involve leading or working as a member of multi-organizational technical teams, where you will carry out a variety of critical tasks, including security requirement definition, system and security architecture development, system alternative analyses, and risk assessments. Qualifications include an MS or equivalent in engineering, computer science, math or a related field, and 7 years' related experience in information assurance. A strong systems perspective and the ability to lead or participate on a multi-organizational technical team are required. Operational experience in military communications, command and control is preferred.

All positions require good organizational skills, excellent oral and written communications skills, and the ability to work independently or as part of a multi-organizational team. Familiarity with DoD sponsors is preferred.

Applicants selected will be subject to a government security investigation and must meet eligibility requirements for access to classified information. US citizenship is required.

APL offers a comprehensive benefits package, including a liberal vacation plan, a matching retirement program, significant educational assistance, a scholarship tuition program for staff with dependents and competitive salaries commensurate with skills and experience. To apply, please email your resume to: [recruiter5@jhuapl.edu](mailto:recruiter5@jhuapl.edu)

The Johns Hopkins University Applied Physics Laboratory is an equal opportunity employer, and we value diversity in our workforce.

For more information about APL, please visit: [www.jhuapl.edu](http://www.jhuapl.edu)

