

# COMPUTERWORLD

## Security

 Print Article

 Close Window

## The Grill: Joan Feigenbaum on 'information accountability'

The privacy expert talks about the problem with encryption, the need for 'information accountability' and what's wrong with role models.

Gary Anthes

**August 25, 2008** ([Computerworld](#)) *Joan Feigenbaum's research interests range from the highly technical to the social and legal aspects of privacy and digital copyright. In 2001, she was named a fellow of the [Association for Computing Machinery](#) for "foundational and highly influential contributions to cryptographic complexity theory, authorization and trust management, massive-data-stream computation and algorithmic mechanism design." She recently wrote about "information accountability" for Communications of the ACM magazine.*

**You wrote that access controls and encryption, which you call "hide it or lose it" mechanisms, are no longer capable of protecting privacy. Why?** The problem with "hide it or lose it" is that people who express the desire for "privacy" often do not mean that they want their sensitive information hidden. Rather, they mean that they want that information to be used appropriately. For example, no one wants the fact that he is a registered voter and a member of the Democratic Party to be hidden from the poll worker who is supposed to put a check next to his name as he walks into the booth to vote in the Democratic primary. Many such voters, however, feel that their privacy has been violated when a Democratic fundraiser uses the same information as justification for calling him at home to ask for a donation. People and organizations should not have to give up the benefits of using information appropriately in powerful networked systems in order to avoid the harms that result when the same information is used inappropriately.

### Dossier



Name: Joan Feigenbaum

Title: Grace Murray Hopper Professor of Computer Science

Organization: [Yale University](#)

Location: New Haven, Conn.

Most interesting thing people don't know about her: "I have voted for two Republicans (in local elections, not national ones)."

Role model: "I don't have one, and I don't want one."

Favorite vice: French fries

Pet peeve: "Co-workers who fail to meet deadlines and then don't even feel guilty."

Ask her to do anything but: "Lie."

**Are you saying that the harm usually comes not so much from the disclosure of private information as from its use?**

Clearly, there are situations in which disclosure of sensitive personal information is considered blameworthy on its face, regardless of the use that is subsequently made of that information. Many people disapprove very strongly when someone talks about details of another person's sex life, for example.

Laws as well as social conventions recognize the appropriateness of secrecy. But those situations are not the interesting ones from a technological perspective. If a particular fact is truly secret, then it's clear what to do: Either do not create an electronic record of that fact or, if you must, encrypt that electronic record.

Technologically, it is much less clear how to handle sensitive information that can and should be disclosed, perhaps to many parties, so that it can be put to beneficial use, but still prevent that information from being put to harmful use. For example, how do we make our consumer preferences available to companies that can use them to improve products but not enable ever more annoying targeted marketing? The challenge is to support appropriate use of sensitive information, not to prevent all use by preventing disclosure.

**You cite as an example of information accountability the [Fair Credit Reporting Act \[FCRA\]](#), which does not limit the collection of credit data but restricts how it may be used.** We could make a great deal of progress toward accountability by facing up to something that many people find counterintuitive: By empowering one or more organizations to collect vast amounts of sensitive information about people while precisely specifying both the types of information collected and the purposes for which the information can be used, we can provide better protection against abuse of sensitive information than we can by constantly warning people to "hide it or lose it."

In exchange for the right to collect and use certain types of personal data, such as credit or medical information, the organizations must agree both to observing the usage rules and to being monitored for compliance with the rules, and they must give data subjects the rights to ensure accuracy of the data and to obtain explanations of decisions made on the basis of that data.

**So could the principles behind the FCRA be more widely deployed?** Absolutely. It would be nice to deploy that more widely. But the whole operating principle behind FCRA is that it would be difficult for the act to be violated invisibly. So the potential Achilles' heel is it assumes that the parties that use the information could actually be monitored. This can be very hard. How can you monitor the use of copyrighted material, for example?

**What are your views in the controversy over [Net neutrality](#)?** I have not yet heard a good definition of the term *Net neutrality*. That's one of the reasons that so much of the discussion about it has been unproductive. I wish that the Net neutrality advocates

would start by stating the problem that Net neutrality solves. Some of them seem to think that there should be a strict separation between the communication function served by Internet service providers and the information-publishing function -- that the proper analogy for a modern ISP is a traditional phone company governed by common-carriage laws, rather than a traditional cable TV company that controls both communication and content.

But what should be required, first and foremost, is that service providers be completely upfront with their customers. They shouldn't imply to their customers that they will be able to use some popular application like [BitTorrent](#), then not actually let them do that. I think it would be great if there were old-fashioned, common-carrier-style ISPs that did no content discrimination whatsoever, but be aware that there are a lot of customers who don't want that.

**You have said you don't like role models. Why?** I don't like the word *role* because it gives the wrong impression that for each person, there's an established path to follow. Each person should seek to live a life, not to play a role. Second, I don't like the word *model* because it gives the impression that if you admire someone, you should try to be like him. I think that's bad advice. A person might be very accomplished and therefore worthy of admiration, but totally unlike you emotionally and psychologically. Modeling your life after his won't work.

*This version of the story originally appeared in Computerworld's print edition.*

*What do you think about information accountability? Let us know in the [article comments](#).*