

# Interview

## Silver Bullet Talks with Annie Antón

**GARY MCGRAW**  
*Cigital*

**A**nnie Antón is an associate professor of software engineering at North Carolina State University (NCSU). She also directs ThePrivacyPlace.org and works on issues surrounding privacy and security. In 1998, Antón was the first Latin-American woman to join the college of engineering faculty at NCSU.

Featured here is an excerpt adapted from the full interview between Antón and Silver Bullet host Gary McGraw. Their conversation ranged widely, from airline privacy policies to end-user license agreements (EULAs). You can listen to the podcast in its entirety at [www.computer.org/security/podcasts/](http://www.computer.org/security/podcasts/) or [www.cigital.com/silverbullet](http://www.cigital.com/silverbullet), and you can subscribe to the full series on iTunes.

**Gary McGraw:** The first question is a doozy, but it's really simple. What is privacy?

**Annie Antón:** Well, privacy means a lot of things to a lot of different people. But I look at that first definition by Warren and Brandeis—the right to be let alone. In today's context, I think it really means that you're able to control information about yourself and reveal things about yourself based on your own decisions, rather than having other people reveal things about you.

**McGraw:** Do you think that Scott McNealy was right when he said that we don't have any privacy, and we should just get over it?

**Antón:** I think that, to a certain extent, he's right. In many contexts, we don't have privacy, but I disagree that we have to get over it.

**McGraw:** That's interesting. As a casual Web observer, it seems to me that most large corporations pay lip service to privacy. Is corporate privacy mostly lip service these days? What have you done to look into that?

**Antón:** It's interesting that you should mention that. We [ThePrivacyPlace.org] did a review of the ChoicePoint privacy breach last year [For more on this issue, please see "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information" article on p. 15 in this issue. —eds] We've made some recommendations regarding what companies should do to protect privacy; what to do about giving notice when there is a breach; what kinds of things they should do, such as regular audits, to make sure that they have a good data-governance strategy; and the things that should be expressed in privacy policies. They should accurately describe the company's overall privacy principles and practices so that they reflect what really takes place.

**McGraw:** Do you think that's common?

**Antón:** We don't think it's common. A lot of times a lawyer writes it with no communication with the people who've developed the systems that really handle the data. Just two weeks ago, one of my students and I spent a whole day at ChoicePoint meeting with the president, CEO [chief executive officer], chief privacy officer, and chief legal officer. They have really taken seriously the sanctions that were imposed on them. I think that they have really turned around from being a glaring example of a company that people didn't know about—and were very concerned about—and probably weren't thinking about the ways in which they were collecting information, and how it affects the public at large, to now completely, dramatically changing their business and their practices.

**McGraw:** But they're still an anomaly.

**Antón:** They are.

**McGraw:** It seems like people find a privacy policy somewhere, and then just copy it or maybe make a couple of tweaks.

**Antón:** That's not what we want to happen. ChoicePoint has really made sure that their policy truly conveys what they're doing. They have dropped some of the clients that

they had because the clients didn't want to go through the extra effort to make sure that they were complying with certain policies that ChoicePoint now has.

I really think it's an example. It's unfortunate that it takes a breach and sanctions for companies to really start paying attention. It seems that ChoicePoint has really become a leader among the data brokers, and they're taking it very seriously. They've cut out portions of their business and are doing a better job of redacting information—even though they don't have to—from some appellate records that are deemed to not be necessary.

**McGraw:** Corporate spankings actually work. You did some work with ThePrivacyPlace.org organization to look at airline privacy policies. What did you find out?

**Antón:** It was really interesting. We called all of the American airlines—we're now calling international airlines as well—trying to figure out what kinds of information they actually discuss in their privacy policies, and whether they could answer questions about ambiguities in their privacy policies.

One thing that's really telling is whether a company has someone at the contact number they provide on their privacy policy—that if you have questions about the policy, you should call this number. With the exception of one airline, they couldn't answer our questions at the number we called.

The one that did was Alaska Airlines, where the gentleman who wrote the policy called us back within about 10 minutes, and answered all our questions to great satisfaction. It's an interesting business model: he's a contractor and works for Alaska Airlines about three hours a week, and then he's on call the rest of the week. They [Alaska Airlines employees] immediately knew who to contact, and it was great.

## About Annie Antón



Annie Antón is an associate professor of software engineering in the Computer Science Department at North Carolina State University (NCSU), where she is also a member of the NCSU Cyber Defense Lab. Her research focuses on methods and tools to support the specification of complete, correct behavior of software systems used in environments that pose risks of loss as a consequence of failures and misuse. This includes Web-based and e-commerce systems in which the security of personal and private information is particularly vulnerable.

Antón is the founder and director of ThePrivacyPlace.org, a research group of

students and faculty at NCSU, Georgia Tech, Purdue University, and the University of Lugano. This group focuses on the development of technology to assist practitioners and policymakers to ensure that privacy policies are aligned with the software systems that they govern. Additionally, she is the cofounder and codirector of the NCSU E-Commerce Studio, a lab in which management and computer science graduate students collaborate in multidisciplinary teams to develop Web-based e-commerce applications for industrial partners.

She is an associate editor for *IEEE Transactions on Software Engineering*, the cognitive issues subject area editor for the *Requirements Engineering Journal*, and a member of the International Board of Referees for Computers and Security.

**McGraw:** Maybe others should try to adopt the same model?

**Antón:** I think so. We called Air Canada and got a voicemail that said that she [the privacy contact] was on maternity leave until September.

**McGraw:** When did you call her?

**Antón:** It was about three weeks ago. And then her voicemail said that if you had any questions to call this other person. So we called the other person. She was on maternity leave until March of next year.

**McGraw:** What does this say about privacy officers?

**Antón:** It's a pregnant pause, apparently.

**McGraw:** Terrible.

**Antón:** I think one of the worst that we encountered was United Airlines, where we had to make three total calls and were transferred three times. We ended up on the phone for 25 minutes with

someone in India. When we asked questions, she said that she wasn't the right person to answer any of the questions, so we asked to speak with the supervisor.

So she put us on hold for two minutes, and came back and said, "We don't share with government agencies or offices because you have a social security number." That's quote-unquote. We then asked her for a corporate office or legal department phone number; she got very agitated and yelled at us.

**McGraw:** Didn't you have one who said you should read the privacy policy?

**Antón:** Yes. When we sent email to Continental, it took them seven days to get back to us. And it was their privacy compliance contact that got back to us and said, "Please review the privacy policy." The first sentence in our email said that we read the privacy policy and had a question. JetBlue Airways took nine days to answer, and also said, "Please review the privacy policy, and if you have questions, we'll be happy to re-

spend. But it's more efficient if you read it first."

**McGraw:** What is the best way to

**Antón:** I don't think the consumers know about it. One of the challenges we have is figuring out the kinds of EULAs that people under-

**McGraw:** One of the things that's happening right now is that Google's attempting to buy Double-Click. Consummation of that deal would produce a huge aggregation of personal data. Do you have any thoughts about that?

**Antón:** Be afraid.

**McGraw:** Is it sort of an unavoidable privacy trend, this aggregation?

**Antón:** I don't see it stopping any time soon.

**McGraw:** I remember a company in the dot-com days that collected a lot of information about its consumers. But when it went bust, it actually sold all the data to make some money for its creditors.

**Antón:** That reminds me of the Toysmart case, where their privacy policy said they wouldn't collect or sell any information. What they got caught for was in their bankruptcy proceedings, they said they would sell their database, and their database contained the names and ages of children. It was a violation of COPA [Child Online Protection Act]. Their parent company—Disney—decided to buy it and destroy the data.

**McGraw:** Fancy that. So it's hard to keep data from aggregating, and there are more and more opportunities for that to happen.

**Antón:** Right, and I think one of the big concerns that people have is that we provide our data for a certain purpose, and we expect it to be used for that purpose. I think the concern—the big privacy concern—is that downstream that data gets used for other purposes that we did not agree to.

**McGraw:** That's because outside of the United States, you own your own personal data, but in the United States, whoever collects it

## I think one of the big concerns that people have is that we provide our data for a certain purpose, and we expect it to be used for that purpose.

impose progress on reticent corporations? Is it regulation, or is it corporate standards?

**Antón:** I think that regulation is a step in the right direction, but one of the problems we're having is that regulations aren't being properly enforced. With HIPAA [Health Insurance Portability and Accountability Act], for example, most of the enforcement is complaint driven, and until there's a complaint, nothing is really enforced.

**McGraw:** I bet most of the complaints are about those forms you have to fill out every time you go to the doctor.

**Antón:** Possibly. But you know, there have been breaches, and I think people file those complaints and the FTC [Federal Trade Commission] investigates, but there's no real mechanism right for enforcing this. The tenet is that we don't have the technology to help companies self-monitor, if you will, for that compliance. That's something that our group here at NC State has been working on.

**McGraw:** When I recently visited NC State and gave a talk about exploiting online games, I talked about EULAs [end-user license agreements]. Do you think customers know about the kind of spyware-based security that is being used by some game companies?

stand and comprehend, and really make sure that they read the EULAs that pertain to the things they most care about.

One of my master thesis students did an experiment where he presented four different privacy policies to people, and then looked at their perceptions about those policies as well as their level of comprehension. What he found was that the perception and the comprehension are really misaligned. People perceive that natural language policies are more descriptive and thorough, and yet they understand them the worst. We found that when you prevent categories of things that are best specified, like notice and awareness or security, that they comprehend the policies a lot better because you're just providing the abstraction.

**McGraw:** I've found that in the online game world, these EULAs are pretty clear. People just don't read it, or they just "click accept." Do you actually read the EULAs of all the software you run?

**Antón:** I read a lot of EULAs. I don't install a lot of software, so I don't normally read that kind of EULA, but I think one of the challenges is, if you present entirely too much information in a EULA, that people don't read it. But if we find out what it is that people really cared about, what are their concerns, and we present those, maybe they'll read them.

owns the data. Do you think lawmakers know that?

**Antón:** I really don't know. It's hard to change something like that when so much information is out there. Recently, I heard someone say we really shouldn't be concerned about this because it's all out there anyway. And I thought, there are future generations for which that information has not yet been developed and we should consider fixing it so that they don't have to deal with this problem.

**McGraw:** McNealy might be right now, but not in the future, not for my kids.

**Antón:** Exactly, right.

**McGraw:** What tools do lawmakers have for negotiating really tricky trade-offs between personal liberty, and privacy and security? Do they have any tools at their disposal?

**Antón:** That's a really good question. I don't know. I do know that the US Department of Homeland Security is trying to develop tools that will enable them to do the kind of identification of folks that should not be coming in the country.

**McGraw:** Like guys with tuberculosis, for example.

**Antón:** Exactly. You know security is as good as your weakest link, so if you have someone who says he looks okay, then he can get in.

**McGraw:** Even though the computer's flashing red.

**Antón:** Exactly. That's not a technology issue; that's a human issue. But frankly, most security problems are because of humans, whether they developed the software that has the vulnerability in it, or whether the folks that use it and have to make decisions based on what information

is in the system. I think that there are attempts to identify people while trying to maintain the information as privately as possible.

**McGraw:** On a completely different topic, what kind of advice would you give to women who are interested in pursuing a career in computer science and engineering?

**Antón:** That's a very interesting question. I've always been really attracted to problems in computer science that have to do with humans, or with things that have an impact on society. And my background, as you know, is in requirements engineering.

Within the field of software engineering, that's the kind of subspecialty where you're interacting with the end users, customers, and the clients, and trying to satisfy all of their different and sometimes competing needs—making sure that you develop the software package that satisfies all of them so that they will enjoy using it. That's always appealed to me, being able to do something where I'm communicating with end users and clients, and then being able to translate that to something that architects and software engineers can actually run with and implement.

**McGraw:** Making computer science more human. You think that'll appeal more to women?

**Antón:** Well, it appealed to me. I don't know if it appeals to all women. The other thing, more recently, is this issue of policy and legal compliance is very interesting to me, especially in the healthcare domain because people are very concerned, and consider information about their medical diagnosis to be very sensitive.

Anything that we can do to help maintain confidentiality in patient records is something that's very appealing to me. I think most women like working in areas where we really do see the impact of our work, and that it's really helping people.

You can find additional podcasts in the series, including those featuring Greg Hoggland and Peter Neumann at [www.computer.org/security/podcasts](http://www.computer.org/security/podcasts) or [www.cigital.com/silverbullet](http://www.cigital.com/silverbullet). □

**Gary McGraw** is Cigital's chief technology officer. His real-world experience is grounded in years of consulting with major corporation and software producers. McGraw is the author of *Exploiting Online Games* (Addison-Wesley, 2007), *Software Security: Building Security In* (Addison-Wesley, 2006), *Exploiting Software* (Addison-Wesley, 2004), *Building Secure Software* (Addison-Wesley, 2001), and five other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. He is a member of the IEEE Computer Society Board of Governors. Contact him at [gem@cigital.com](mailto:gem@cigital.com).



**FREE Visionary Web Videos about the Future of Multimedia.**

**Listen to premiere multimedia experts! Post your own views and demos!**

**Visit [www.computer.org/multimedia](http://www.computer.org/multimedia)**



**\$29**  
New Lower  
Subscription Price!

IEEE  
**SECURITY & PRIVACY**

Subscribe to our  
magazine today  
for only \$29—  
our lowest price ever!

You'll receive 6 issues of today's  
leading-edge, peer-reviewed  
software development information.

Ask us how  
you can get this great deal on  
*IEEE Security & Privacy* magazine!

*S&P* is the premier magazine  
for security professionals.  
Every issue is packed with  
tutorials, best practices, and  
expert commentary on:

- attack trends
- cybercrime
- security policies
- mobile and wireless issues
- digital rights management
- and much more.

Subscribe at [www.computer.org/services/nonmem/spbnr](http://www.computer.org/services/nonmem/spbnr)