

If Your Privacy Matters To You...

Thank you very much for inviting me to speak with you today.

I was originally asked to give a talk that I'd given a few months ago to the New Jersey Technology Council. That talk was called *The Second Information Age*. The NJTC is a pretty high-tech audience, as you'd expect, and in that talk I tried to identify several really high-level trends in information technology.

My takeaway message was that folks are going to be a lot more skeptical about technology in the coming years than they *have* been up until now. OK, what kinds of problems are people really going to want technology to solve? What kinds of information and communications technologies are most likely to solve the problems that people care about most?

That's what I was *going* to talk about today, too.

But last week, someone who's here today put a bug in my ear about some things that have been on my mind anyway, that have been all over the news. So I decided to talk about that instead -- and I hope you'll find what I have to say a little more timely, more relevant to you.

If you're interested in what I was originally planning to talk about, Deb Di Gregorio from Camares Communications, who's in the back, has copies of *that* talk. So you can actually get two talks for the price of one.

What I'd like spend a few minutes with you on today is electronic commerce. More specifically, I want to talk about the one word that I believe is at the heart of success with electronic commerce.

The word is *trust*.

I hope to convince you that trust in e-commerce is important to *you*, personally -- whether you're directly involved with building your company's Web site or not.

That it's important to you even if you're a customer, or simply a citizen in a world that really *is* being transformed by the Internet.

You know how important trust is in your real-world business relationships. We've all dealt with people we don't trust, and you know what it's like. As soon as you realize you don't trust your business partner -- or as soon as you have a choice -- you're outta there. Trust is really the foundation of any business relationship -- *any relationship at all*.

Now, what does trust mean online, on the Internet? Where you can't look in someone's eye, shake their hand? Where you may not have a salesperson who can put in a good word with the boss, do you a favor, fix a problem with last week's order?

The best definition I've heard comes from a team of e-commerce experts at IBM. In a book called *Electronic Commerce Relationships: Trust by Design*, they say trust in e-commerce has three elements:

Certainty. Confidentiality. Privacy.

Certainty is reasonably easy to understand. When you attempt a transaction, is it completed? Is your merchandise actually delivered when it's supposed to be? Did you get the quality you were expecting?

And, of the three, certainty *may* be the easiest for a competent e-business to deliver. You build an electronic shopping cart that always tells people exactly where they stand in the buying process. When they're done, you send them an email confirmation. You give them package tracking information, so they can see exactly where their stuff is.

The hardest part, especially if you're a *large* e-business, is to build fulfillment processes that *work*. But, increasingly, you can outsource much of that, so at least you don't have to reinvent the wheel.

The other two elements, *confidentiality* and *privacy*, are far more challenging -- and they're what I *really* want to discuss with you today. They're intertwined, so I'm going to discuss them together.

Imagine, for a moment, that you and I have just met. Maybe, down the road, we *might* do business together.

You invite me to your place of business, or perhaps your home, to get to know me a little better. You want to see what I might have to offer.

On my way over, someone buttonholes me. They say to me, I have this tiny little black box. I see you're on your way over to Bob's house. I'll pay you X, if when you get there, you'll simply leave this box in some corner, somewhere, where Bob and his family won't notice it.

And what does this box do? Well, it's got a little transmitter in it. It'll keep track of where Bob goes. What he's interested in. What he buys.

But don't worry. Most folks never realize it's there. Chances are, Bob won't either.

So what are you thinking when you're listening to this guy?

Well... times are a little tough. My investors have poured millions of dollars into my business. They want to see a return. This would be a *wonderful* revenue stream. I could leave one of these boxes at *everyone's* house I visit. I'd hardly need to sell a thing!

Is that what you're thinking?

I sure hope not. Why not?

Because you know, and I know, that it would be a personal betrayal of your customer to do this. You wouldn't want someone to do it to you. And if you don't happen to be guided by those particular ethical principles, there's always the chance you might get caught.

Now let's take this onto the Web. Some of you are way ahead of me, and you know where I'm going.

There's something called a cookie, which is sort of the equivalent of that little black box. When you visit a Web site, the site leaves a cookie on your computer. Many of these cookies are perfectly innocuous. They just help the site remember you. (That's why when you go back to Amazon.com, it says, "Welcome back, Bill. We think you'll like these selections...")

But, increasingly, cookies are being used for much more than that.

If you look behind the banner ads served by many sites -- including many e-Commerce sites -- you'll see they don't come from the same place as everything else on the site. They come from an advertising company, such as DoubleClick, which brings together information from *all* the sites it works with.

DoubleClick cookies can be remarkably powerful, because they can track the behavior of people at all the sites DoubleClick works with. That's over 11,000 sites. Many of them extremely large -- such as the *New York Times* and *Sesame Street*.

To give you a sense of DoubleClick's scope, they serve over a billion banner ads every day. They're the McDonald's of Internet privacy invasion.

Well, OK. All of this is anonymous, right? It used to be.

Previously, it was only possible for DoubleClick to track anonymous profiles -- they'd know *somebody* visited all these sites, and *somebody* should receive Targeted Ad "X" -- but not who that somebody was.

That's changed. Last fall, DoubleClick bought Abacus Direct, one of the world's leading mailing list managers. They've got files on 90% of all American households. Now, DoubleClick has started encouraging its Web site partners to share your name with them. Once they have it -- *just once* -- they can link your cookie with their Abacus databases. And *then* they know more about you than you might ever imagine.

Here's how it works, courtesy of *USA Today*...

?? DoubleClick sends a cookie to your browser and gives it a unique ID number.

?? DoubleClick sends the same ID number on to the site that knows who you are -- *maybe you registered there, or bought something*.

?? That company then sends back the data that DoubleClick needs to look you up in the Abacus database.

?? And voila -- DoubleClick knows who you are, too.

So far, only about a dozen sites have bought into this deal -- but all it takes is one.

DoubleClick won't tell you who's signed up. The sites themselves are supposed to tell you. But so far, *nobody* seems to know who they are.

So, one day, you browse to a financial planning site, and next week you start getting junk mail from brokers...

Or... you read an article about mental illness and suddenly you start getting mail about Prozac...

Or... suddenly, some very suspicious riders start appearing on your health insurance policy...

In fairness, DoubleClick says that health information is off-limits. But last year they *also* said they weren't tracking individual user names. Well, one day, they changed their minds. Who's to stop them from changing their minds again? Who's to stop one of their competitors? They're not the only folks in this business.

Also in fairness, DoubleClick says people can opt out. Do you read all the small print on every site you visit? Should you have to? When you change computers, or switch browsers, you get a new cookie -- do you have to opt out all over again? Who knows?

I'm *in* marketing. And I must tell you, having the power to track people this way is pretty amazing. It's awfully tempting.

But power comes with a price. And that price is the trust of your customers.

Nobody trusts a blabbermouth.

But if you don't know *who's* spying on you, or how, what's your natural reaction? *Don't trust anyone.*

You go to a site, you happen to notice that its cookies come from DoubleClick... and you wonder. Are *these* the guys who are gonna sell me out?

It's not the way you *want* people to be thinking when they visit you on the Web.

What's worse, the people you want most as your customers -- the aware, educated, well-off consumers who pay the most attention to this stuff... *those* are the ones you're most likely to lose.

Many enlightened e-commerce executives are coming to realize this.

Recently, the *Internet Data Market Report* took a small random poll of e-Business executives. 68% said DoubleClick's new program would have a negative impact on e-commerce. And when asked whether consumer concerns over privacy were holding back growth in their e-commerce markets, 44% said either "considerably" or "somewhat". Only 1 in 8 could say it was having no impact at all.

Now, I've been focusing on DoubleClick, because they've become the poster child for this stuff. But they are far from the only offender. And cookies are *far* from the only way your business can invade folks' privacy -- even if you're not intending to.

Remember MCI's *Friends & Family* program? Well, British Telecom -- which is suddenly facing plenty of competition, too -- thought it was a pretty neat idea. So they sent out a huge mailing. *Here's the number you call most often -- why don't you sign up with our program, and those calls will be free!* Guy's wife opens the envelope... Hmm... I don't recognize that number... next thing you know, they're in divorce court.

Or, one large HMO -- with the best of intentions -- tried to help diabetics get the preventive care they need to avoid eye damage. So it sent a *Dear Diabetic* letter offering free retinal eye exams. But as you may know, there's a form of diabetics that affects pregnant women, called gestational diabetes, which usually disappears after a woman gives birth. A woman got this letter, thought it meant her diabetes had returned. She panicked. You know what came next: the lawyers.

I'm simply asking that you think even more carefully about these issues as you do business. And *especially* as you do

marketing on the Internet, since it's such a powerful medium for targeting individuals.

I certainly don't have all the answers, but I know where to start. You do, too. *Put yourself in the shoes of your customers.*

The most powerful tools are the ones that are the most likely to backfire on you. One day soon, it'll be revealed who is sharing their names with DoubleClick -- and I guarantee you, making that decision won't turn out to have been such a great career move!

I'm also asking you to think about the impact of these technologies on our lives, not just on our businesses.

There's a scary new book out, called *Database Nation*. And in it, the author -- Simson Garfinkel -- makes the point that privacy isn't just about hiding things.

"It's about self-possession and integrity... It's about lovers who will take less joy in walking around city streets or visiting stores because they know they're being photographed by surveillance cameras everywhere they step... It's about good, upstanding citizens who are now refusing to enter public service because they don't want a bloodthirsty press rummaging through their old school reports, computerized medical records, and e-mail."

Some people say privacy is a lost cause. Or, as Scott McNealy put it -- he's the president of Sun Microsystems, the folks who make the servers that run the Internet... you know, "the folks who put the dot in dot.com"... "You have zero privacy anyway. Get over it."

I wanted to call him to complain, but for some reason, he has an unlisted number.

Some people say we'll all be better off living in a transparent society. That it'll ultimately be more liberating. Since nobody can *have* a secret, nobody will *worry* about secrets.

If you agree, do nothing -- because that's where we're headed.

If you *disagree* -- if your privacy matters to you -- now's the time to act, as businesspeople at work, and as citizens in the

community. Personally, I don't think it's a lost cause. Awhile back, Lotus planned to introduce a CD-ROM called Marketplace, which was intended to contain information on 80 million households, including names, addresses, shopping habits, likely income levels, and even a categorization into one of 50 categories like "accumulated wealth", "mobile home family", "cautious young couple." All for \$695.

It would've been a wonderful marketing tool, especially for small businesses. But would you have wanted your *neighbor* to be able to do a search that led them straight to *your* record? The outcry was so loud, the product was cancelled.

So it really is, ultimately, up to us. I hope you'll agree with me that it's time we stood up for the privacy we still have. While we still can.

Thank you very much.