Remarks by Michael Eisen, Microsoft Canada Co.

to

3rd Annual Privacy and Security Workshop
11th CACR Information Security Workshop

PRIVACY AND SECURITY: TOTALLY COMMITTED

University of Toronto
November 7-8, 2002

Thank you and welcome.

In my talk with you this evening, I've decided to return to first principles.

I want to begin by asking – Why is privacy so important? Are we really worse off if an increasing amount of our lives is recorded, sifted through and analyzed? If we are typical, law abiding citizens, why should we be particularly concerned about maintaining our privacy?

A recent essay in Maclean's magazine asked these very questions. Entitled "Privacy: Who Needs It?" the piece identified all the benefits we could gain from having less privacy:

- A reduction in crime if we were able to track people's whereabouts through chip implants.
- Real time monitoring of our vital signs to ensure better health.
- The ability to break up conspiracies and terrorist threats before they get any real traction.

Think about it for a second. Do we really need more privacy, or even as much as we have? Especially, if arguably, there are clear benefits, either for individuals or the whole of society, from making our lives somewhat more public?

Put another way . . . Is privacy an outdated holdover from a different time – a time when some democracies, notably the U.S. under Nixon, appeared ready to trample people's rights for their own partisan political purposes? Have we been brainwashed by writers like George Orwell and Margaret Atwood into thinking any loss of privacy will lead to totalitarianism? Or is privacy simply incompatible with our new, digital existence?

Scott McNealy, CEO of Sun Microsystems, made this blunt pronouncement on trying to preserve some abstract notion of privacy. "You have zero privacy anyway, get over it."

Well, not for the first time . . . or the last, I suspect . . . I disagree wholeheartedly with Scott.

I believe that privacy is one of the building blocks upon which democratic societies are built. Knock out part of the foundation and the whole structure is a little less stable. Disrespect and invasion of privacy are the hallmarks of tyranny.

Privacy, in one form or another, is enshrined in our constitution, recognized by the common law and, more recently, the subject matter of legislation.

The federal Privacy Act and the office of the Privacy Commissioner were established specifically to protect the personal information held by government institutions. They also provide individuals with a right of access to that information.

Under Bruce Phillips and now George Radwanski it's been a busy place. The work load has increased substantially since January 2001 – when the Commissioner became the privacy watchdog under Bill C-6.

Of course, we're fortunate to have you, Ann, leading the charge here in Ontario, sponsoring conferences like this one and working hard to help the Ontario government draft new legislation that meets the emerging needs of the digital era. You've been a great force in communicating to individuals about the importance of privacy – through speeches and in your recent book entitled "The Privacy Payoff: How Successful Businesses Build Customer Trust."

All this activity is occurring for a reason – Anyone who thinks that modern democracies have moved into some "mature" phase where basic protections are no longer necessary has a very shortsighted view of history.

Democracy, the rule of law and a commitment to the protection of individual rights, while exceptionally resilient in most western countries, are in fact fragile concepts. That they persist and work at all is a testament to the amazing forethought of our founders and the strength of the institutions they created.

But more than that, democracy and the rule of law survive because their key tenets have become embedded in our values.

So this is why Mr. McNealy is dead wrong – Sure some privacies are being eroded, but responsible people don't throw open the barn door because one horse has bolted!

Responsible people rise to the challenge when someone starts striking at the foundations of our democracy – and threats to privacy, whether through benign erosion or malicious attack – are exactly that.

- - - - - -

Accepting then that privacy is a core value, I want to talk a little bit about why I think it's of paramount importance right now. I believe that as a society, we've reached a "tipping point" where concerns about privacy, security and technology could soon – and quickly – become of paramount importance to people.

In his book "The Tipping Point: How Little Things Can Make a Big Difference," Malcolm Gladwell investigates moments of dramatic, often seemingly inexplicable change. We've all witnessed these kinds of changes – the mass adoption of a new technology like cell phones or fax machines, a dramatic rise in teen smoking.

What is it that causes these things to “tip” or explode from slow, gradual growth to something that more closely resembles an epidemic?

Gladwell argues that these trends can be explained in *exactly* the same way we explain epidemics. Ideas, products, messages and behaviours all spread the same way viruses do. Sometimes they spread steadily and slowly and sometimes they spread through outbreaks. Ideas and behaviours, argues Gladwell, are as susceptible to outbreaks as viruses are.

Two of the key characteristics of an epidemic or outbreak are that seemingly small events can have very large effects and that they can happen very quickly.

Small events having large effects is a difficult concept to grasp, because most of us tend to think in terms of cause and effect. We think that whatever goes into one side of a transaction is pretty close to what comes out the other side. But this isn’t the case with epidemics.

Small issues can bubble under the surface, where no one pays attention. They can come together in ways we never imagined, like a strange chemical reaction. Or maybe one small problem moves *just* past an unseen threshold and suddenly, a fashion trend is born or public opinion turns 180 degrees.

Epidemics and crises seem to occur out of the blue – but they don’t. It’s just that most of us don’t know how to see them coming.

I believe that those of us working on privacy and security challenges can learn a lot from Gladwell’s theory.

Generally speaking, things are going fairly well. We’re all reasonably sensitive to the importance of privacy. Responsive legislation is being drafted and implemented. The technology is improving every year.

Nevertheless, I still believe that if we don’t address privacy and security issues correctly now we could “tip” into a situation that would be far more difficult to correct down the road and one that could have devastating consequences for business.

One of the problems that is simmering and may boil over is precisely that our ability to protect the value people put on privacy may not be keeping pace with technological change.

Let me explain by quoting Bill Gates!

Bill Gates has often said that we are now entering what he calls the Digital Decade. At its core, the Digital Decade is about the idea of computing being woven much more deeply into the fabric of society and our workplaces.

We tend to think that computing is pervasive now, but it really isn't – we still use computers mostly for discreet tasks, many of which we could perform in some other, non-computer way – sending mail, writing documents, keeping track of inventory, landing planes at airports, building cars, etc.

Computers make all of these things easier and faster, but we could still do them without computer assistance.

Bill's vision of the Digital Decade is one where computing moves from these discreet tasks to a more pervasive presence in our lives. He's talking about a time when computing just happens in the background – letting us focus on the task at hand, and also a time when computing is a much more personal experience; one where we configure the digital world around us for our benefit.

The other important element of the Digital Decade has to do with the pace of change. Not only will computing become a more seamless part of our lives, but the rate of technological change is accelerating at an almost exponential rate. Bill believes that the technological advances of the first decade of the 21st century – this Digital Decade – will dwarf those of the last 40 years.

If the world is going to change as much or more between now and the year 2010 as it has since 1960, we are in for nothing short of a revolution.

However, if we are to see the power of computing unleashed; if we are to gain all the benefits we can from it, people's ability to innovate cannot be held back by our failure to live up to society's expectations for personal privacy and security.

This is why Microsoft has embraced a Trustworthy Computing initiative. Richard Purcell, Microsoft's Corporate Privacy Officer from Redmond, may very well talk more about the nuts and bolts of Trustworthy Computing tomorrow. What I want to talk to you about right now is the magnitude of Microsoft's commitment to the cause, because I think it says a lot about how important we think the issue is.

Trustworthy Computing is bigger than just privacy and security. If computing is to become ubiquitous, like electricity, the phone service, gas and water, then it needs to be as secure, safe and reliable as these other services. Computing needs to function like a utility – we need to trust it for more than just the tasks we can replicate without computers.

But our water pipes and electrical lines don't carry our credit card numbers or collect our personal information. With ubiquitous computing comes even bigger security, reliability, availability and, privacy challenges.

And overcoming these challenges is left to all of us.

For our part, we’re in the process of training all our developers in the latest secure coding techniques.

And most importantly, we are committed to making security, privacy and reliability paramount. In practice, this means that now when we face a choice between adding features and resolving security issues we need to choose security.

Now, I’d like to return to the notion of the tipping point that I mentioned a few minutes ago. All of us have accepted, I think, that privacy is an important part of most people’s value systems, one that few of us want to see eroded, and one that businesses ignore at their peril.

We’ve also discussed what’s coming in the digital decade when not only will the pace of change accelerate at a rate that we’ve probably never seen before, but our relationship to computing will change. It will become more personal, which brings many benefits, but it will also become more transparent and pervasive, making most of us more reliant on computing and the technology that underlies it than ever before.

Lastly, we’ve discussed the challenges to making computing trustworthy – challenges that span the entire industry and that we feel require unprecedented cultural changes within companies.

These two sets of factors – the digital decade and the work the industry has to do on privacy and security – run parallel to one another and are completely interrelated. To succeed at one, we must succeed at both, and we must do it now, because the pace of innovation is not slowing.

At best, if we fail to move aggressively on issues of privacy and security today, we will limit the benefits of the Digital Decade because our inability to keep the public’s trust will work like handcuffs on those who are working on tomorrow’s innovations.

At worst, getting it wrong could forever destroy public trust. This would not help anyone’s business, it wouldn’t help the economy, it wouldn’t be good for democracy.

So, what can we do to make sure we all benefit from the great potential of the Digital Decade?

- - - - - -

There’s a point I’d like to make here. Although technology will make a critical contribution, alone it will not provide a complete fix to the privacy protection challenge. Rather, we also need a paradigm shift in personal and corporate attitudes.

A recent Economist article cited surveys in which two-thirds of British commuters at London’s Victoria Station were willing to reveal their computer password in return for a ballpoint pen! More troubling, the Meta Group notes that the most common way for intruders to gain access to company systems is not technical – they simply find out the full name and username of an employee, usually through an email, and call the help desk and say they’ve lost their password.

And lest you think the problem is limited to individuals working in small businesses, Gartner has quoted the U.S. Defense Security Service as saying that the most common approach foreign nationals take to acquiring U.S. military secrets is to pick up the phone and ask for the information.

The lesson is this – many of the challenges we face in protecting people’s privacy and security are profoundly human. They are about changing the way we behave, which is not easy when we’re all on the steep learning curve associated with technological innovation.

Those who would violate your security or privacy know this: To quote one security expert “amateurs hack systems, professionals hack people.”

So, how does a person protect their privacy in the digital age?

First of all, it has to be easy – and that is partly our responsibility. There’s a reason beyond laziness that people choose passwords they can remember. We simply can’t remember a dozen different passwords of at least eight characters each, including punctuation and numbers. And no amount of scolding from the “experts” is going to change this.

Second, people need to understand what kind of digital information needs to be protected and the consequences of revealing too much. I would hazard a guess that if the people who gave out their passwords for a pen were asked how they felt about protecting their personal privacy – most would rate it as a high priority.

Some experts believe that privacy is a non-issue for the general public – citing studies like the pen giveaway to prove that people don’t care; that privacy is not top of mind.

But they could be measuring the wrong thing – they could simply be measuring people’s perceptions of the danger. If people don’t understand the risks and can’t make the connection between giving up their password and, say, identity theft, then these studies are useless.

I believe that people want to protect their privacy. I believe that for most, it is a cherished value and people are usually willing to take some of the responsibility for protecting their values. But people are frustrated, confused and not sure where to start. And all the while, every breach makes them feel more violated and we lose a bit more of their trust.

That’s often the way people react after their home has been broken into. But people have some idea of how to protect themselves from a home break-in by using better locks or security systems. They also know what to do if they’re broken into – call the police or trip the alarm. And they know what their rights and remedies are when they are robbed.

But what about companies and other organizations? How do they build a culture of respect for privacy? How do we convince employees not to use their pet’s name as their password? Not to stick post-it notes containing their passwords to their monitors or not to tape them under their keyboards? To log out of their systems before they leave for lunch or, worse, at the end of the day?

Clearly, we must focus on education as well as technology.

EDS, for example, makes all employees take a regular onscreen test to ensure they understand the company’s policies on passwords, viruses and network security.

At Microsoft, over the last little while, we have been rolling out a Privacy Health Index to help institutionalize privacy best practices at the company.

With the understanding that you cannot manage what you cannot measure, we have built a complete suite of privacy tools including a Privacy Handbook and supplemental online training.

Our divisional managers are being tested on their team’s privacy comprehension and given a score that represents their group’s performance. Finally, by building this Index into organizational business review cycles, we hope to identify areas of improvement and raise the level of privacy understanding across the company.

We think these kinds of measures should become as important within an organization as measuring productivity and management skills. They must simply become part of everyone’s routine.

Before leaving to participate in what will undoubtedly be two days of informative discussion and debate, I just want to encourage us all to keep first principles in mind. Privacy matters – it matters because we are worse off without it and because business will suffer immensely for not learning this lesson.

And while we are well underway in transforming the way we work, live and play in the 21st century; while we are undoubtedly poised to reap amazing benefits from the Digital Decade, I think we have a long way to go to ensure that our traditional values are protected in the digital era. I also think we’re up to the task. I hope you agree.

Thank you.