Piracy on the PCs—Remarks by Carol Bartz, Chairman and CEO, Autodesk, Inc.

To:
The Commonwealth Club of California
November 18, 1996
Palo Alto, California

Good evening.

I'd like to begin tonight by asking you to imagine a situation. Let's say that you work for a company that manufactures personal computers. You decide to go into work on Saturday to clean up a few projects.

While you're working in your office, you see a truck enter the parking lot and go to the back of the building. "That seems odd," you think. You investigate and see men loading boxes from the warehouse into the truck. You call the police and when they arrive, they arrest thieves who are stealing newly-manufactured PCs from your warehouse. Later, you find out it's been going on for weeks.

How do you feel? Well, you're upset and you're mad. You say, "The people here have worked a lot of hours to fill that warehouse. And the sales of those products are my paycheck."

Now you know what it's like be in the software industry.

Thieves steal billions from us every year. And they get away with it year in and year out. Software theft runs the gamut from full-fledged counterfeiters to people who copy a few floppy disks.

The software industry is one of the crown jewels in the U.S. economy. It's a real American success story.

We're good at software. Our innovative, just-do-it culture seems to grow new programs and new companies. In the process, we've created—not just hundreds of thousands of new jobs—but whole new industries.

Annual sales of software are close to $75 billion a year. That's three times bigger than the movie industry.

Software touches all of us every day—even if you never use a computer. Software is at the heart of everything from the traffic lights in your home town—to the MRI machine in your community hospital.

It runs the pumps at the gas station and the cash registers at the supermarket. It's used to design the cars we drive and the buildings we work in. It even calculates and prints your paycheck.

And—I don't want to be presumptuous—but without software, our nation's investment in computer hardware is worthless.

There's no question that the U.S. software industry has a bright future. The explosive growth of computer processing power will create software opportunities in the next decade that we can barely comprehend. And the growth of the Internet will create even more opportunities.

But the software industry in the United States has a major problem. It's called software theft. Theft accounts for $15 billion in lost revenue each year. That's 20% of total sales.

Because Autodesk makes complex, expensive software, our theft rate is much higher. We estimate that there are eight illegal copies of AutoCAD for every legal one. The media often calls software theft by the wrong name. They call it "piracy." I don't much care for the name "piracy." It conjures up images of Errol Flynn and swashbuckling adventure movies.

What we're talking about isn't romantic. Stealing software is no different

from using a crowbar on the back door of the local appliance store and taking a couple of television sets.

Software theft is not a victimless crime. It slows down an important U.S. industry. It short cuts jobs and taxes. If you have a retirement plan or 401k that invests in high tech stocks, you're also a victim.

Some people justify software theft by saying that these companies make too much money. Well, not everyone is Bill Gates. Many software companies are small, struggling groups that depend on the revenue stream to stay alive. Often, developers have used all their savings and maxed out their credit cards to create a program. For larger companies—such as Autodesk— developing a new program means a very big investment. And we've got to make the total investment before the first dollar of sales comes in.

Software thieves say, "It's a small thing. Look how easy and inexpensive it is to make a few disks."

But making software really isn't about disks. Making software is about people. A new program can take hundreds of people each working thousands of hours to create the content on those disks.

One of the biggest problems we have in fighting software theft is this perception that it's not really stealing. Here's an example.

There's a small software company in California called Abacus Concepts. They've developed an award-winning program called StatView. It's used to analyze statistical data. A lot of people save time using StatView—and sales are very good.

What a great American success story. This group of 25 people develops a great program—and they reap the rewards. Well, not quite.

Abacus Concepts has sold 75,000 copies—but they estimate that there are more than half-a-million illegal copies in use worldwide.

Recently, they discovered a customer in Sweden who was using hundreds of illegal copies. Here's the kicker—and it shows why software theft is a perception problem. The customer is the Karolinska Institute in Stockholm. It's a prestigious medical research organization. And they happen to be the people who give the Nobel Prize for Medicine.

When these scientists describe themselves, is "felon" the first word that comes to their minds? Probably not. And that's our perception problem in a nutshell.

Let's look at who steals software. First, there are a small number of professional counterfeiters. These guys are crooks and they know it. They run assembly-line operations—copying and selling bogus software— complete with authentic-looking packaging. This is a worldwide phenomenon. It stretches from illegal CD-ROM factories in China to the streets of Los Angeles.

The volume counterfeiters get a lot of headlines—and they are a problem. But they're not the big problem. The big problem is what we call "soft lifters." They're often business people who make illegal copies of software for their own use. They may have one of two legal copies of a desktop publishing or word processing program. When it's time to add more computers, they just copy the software.

They say to themselves, "Hey, I already bought the program. What's the harm?"

The harm is that—taken together—they're responsible for 80% of all software thefts. That's about $12 billion dollars a year.

A third group of software thieves I call—sadly—the "grandmothers." Grandmothers represent the casual thieves who copy a few disks. I know that I'm taking a hard stand on grandmothers. But I'm doing it to make a point. Casual thieves often don't even realize that they're stealing.

It happens like this. It's Christmas time—and a grandmother is shopping for

presents for her grandchildren. She buys one copy of each computer game. Then grandpa sits down at his computer for an hour with a box of blank floppies—making copies for each of the grandchildren. Then grandma wraps each gift in fancy paper with a nice bow. It's not likely that the tag will say, "I hope you enjoy this stolen gift. Love, Grandma."

Software companies like Autodesk work hard to prevent theft—but it's an uphill fight. In the 1980's, the industry tried putting software locks on floppy disks. But this was an impractical, unworkable solution—and it was abandoned. There are a lot of ideas floating around for preventing software theft—but they're still complex and cumbersome.

And the software industry faces new threats from new technologies. New storage devices—such as digital video discs and user-made CD-ROMs—will give thieves an even bigger edge.

The growth of the Internet provides another way to steal. We call it the "The Home Shoplifting Network." The Business Software Alliance is an industry group made up of companies like Autodesk, Microsoft and Novell. It works to control software theft by focusing on enforcement and public policy.

Through the Alliance, the software industry works to influence legislation. This is sometimes a tough sell. The technology is complex. It changes quickly. And often, legislators aren't experienced computer users.

A third focus of the Business Software Alliance is education—teaching people what constitutes software theft. And as the Nobel Prize folks in Sweden show us, we have a long way to go.

Tonight, my goal is to educate. I've got a bully pulpit with a million radio listeners—and I'm going to use it. I want to change the perception of software thievery. To start, I want to take you to the scene of the crime.

Software theft takes place in cyberspace. Someone called it, "Everywhere at once and no particular place at all." We can think of cyberspace as starting at your personal computer and extending outward from there. It's a collection of hardware and software technologies and communications channels.

But it's also a new social space—where people interact.

When you enter this new social space, you notice that the rules are—well, a little different. A lot has been written about the emerging cyberculture. Some call it "the online world" or "the wired world."

If you read Wired Magazine you know what I mean. Cyberculture is hip, irreverent and edgy. It's eager to shock—with both words and images.

You could say that the online world is now in its unruly, adolescent stage. In some ways, it's like the Wild West all over again. Think about frontier towns in the West of 150 years ago. These towns were new social spaces—where a lot of the old rules didn't apply.

People wore guns for good reason. Cattle and horses were stolen—and claims were jumped. Shootings were common.

Of course, not everyone was a lawbreaker. But the culture was defined by what a few people got away with—without being punished.

Cyberspace is our new frontier—and cyberculture is our new Wild West. We've even invented new words to describe new kinds of uncivilized behavior. Like "flaming"—which is launching an all-out personal attack, often anonymously. And "spamming"—which is sending unsolicited messages to thousands, or even millions of email addresses.

In the online world, sometimes we hear the rhetoric of anarchy. We hear that this anarchy is a key element of the new culture.

I don't buy that.

Let's face it—there are people who like anarchy. They're like the ones who moved to the Wild West—for all the wrong reasons.

The online world is now going through a process of socialization.

Eventually it will settle down.

Our goal should be to hold onto its freshness, energy and innovation. And lose the amoral, antisocial and illegal parts.

As this new culture becomes more mainstream, it will reflect accepted rules of law and civilized behavior. A hundred and fifty years ago, you could wear a six-shooter right here on the streets of Palo Alto. I wouldn't recommend it today. This town has changed from the Wild West to the Mild West. Or maybe we should we call it the Mellow West.

To bring the online world into the fold, this new social space needs to be civilized. This is important because it's getting bigger at warp speed. And it's a place that we're going to leave to our children. It's one of the places they'll live and work.

To every generation falls duties and obligations. Our grandparents and parents had to deal with the Great Depression and World War Two.

Our generation will be the ones to civilize cyberspace. One of the first steps is to make it honest. And a great place to begin is to stop stealing software. The Wild West started to become livable when people stopped stealing horses regularly.

There are good, practical reasons to reduce software theft. It holds back jobs and growth in one of the most successful and promising U.S. industries.

In the next century, nations will compete more on the economic playing field—and less on the battlefield. Software gives U.S. industries powerful competitive advantages.

We design cars and airplanes faster and better because of software. We spend less on things like inventory and distribution because of software. We can communicate words and pictures around the world in an instant because of software.

As a country, we're going to need every competitive advantage we can get in the global arena. A strong and vibrant software industry will be a big plus. Software thieves are not only stealing today's software.

They're stealing the future.

They're stealing the next generation of more powerful, easier-to-use software.

One of our big challenges in the industry is to make software more enjoyable and more intuitive. That takes a lot of R&D investment and some pretty advanced thinking.

But R&D budgets can only come from one place—product sales.

Software thieves are also stealing tomorrow's opportunities. There are people who would love to develop programs for the classroom—for instance, one to teach geography to fifth graders.

These clever designers would combine multimedia technology with proven educational concepts. Their goal would be to entertain while they educate.

But the truth is that programs like this just don't get developed. Venture capitalists readily admit that they're reluctant to put money into software development for the school market.

The problem is that teachers buy one or two legal versions—and then copy disks like mad. And they say, "It's for the kids."

Please don't misunderstand. I'm all for use of software in the classroom. Many software makers—Autodesk included—have special educational pricing. And we donate software to schools.

The real tragedy here is the worthwhile software that never gets developed. Nobody's going to put a million dollars into a product for a market where theft is commonplace.

Here's another reason to be on the right side of the software theft issue.

It has to do with instilling sound values in our children. If you're a parent of growing children, you're very conscious of being a role model. Our kids

watch us like hawks—and they don't miss much. As a parent, when you have a chance to impart a life lesson, you take it.

Let's say you take your 10-year old to the mall. As you walk out of a store, you notice that your youngster has a new toy—which is a little suspicious. No store bag and no receipt.

You ask a few questions and the distraught look on the child's face tells the whole story.

So you march your kid back to the store and make him face the music. You both find the manager. With tears in his eyes, your child explains that he took the toy without paying for it. And that it was a mistake. And it will never, ever happen again.

You and the store manager nod with approval—and the incident is closed. But not without an important lesson being learned.

OK, let's flash forward two days.

Your child sees you sitting at your PC. You've got a new software program and it's already-opened box.

Your child says, "New software, dad?"

"Yes," you mumble.

"Isn't that the one that Jeremy's dad got last weekend?" he asks.

The look on your face tells the whole story.

"Why are you copying that?" he asks.

Your mind races through the available rationales. "It's not really stealing if you don't get caught." "The company makes lots of money anyway." "I really need this."

All of them sound terrible. You know why you don't have a good answer. Their isn't one. You know that there's no difference between stealing the toy and stealing the software.

Aside from pragmatic considerations, there other reasons to stop stealing software.

I'm going to do something old fashioned.

I'm going to appeal to your sense of honesty and decency—with a moral call to action.

Don't steal software. And don't condone it.

If you're the owner of a business—big or small—you need to have a written policy on illegal software. And you need to enforce it.

To the casual thieves—the grandmothers—I say this. When a person copies software, it make them a thief. If knowing you're a thief bothers you, the remedy is simple. Don't do it.

I know that not stealing software is hard to do. It's so easy. And who's to know? It's an invisible crime. Electrons moving from one place to another. But a single theft multiplied millions of times has an enormous impact on the software industry.

Software theft is not a victimless crime. When you steal software, you're stealing from me.

More importantly, you're stealing from people who work for software companies. And you're stealing from their families.

Yes, stealing software is common in today's cyberculture. It's as common as stealing horses was in the Wild West.

But the situation has to change. When the bad guys win—and hard working, honest people lose—there's something wrong. It's the wrong value system. And wrong value systems on a massive scale are dangerous. They send the wrong messages. And they encourage the wrong behaviors.

Cyberculture is going through its growing pains now. It's our job to make it a place where we want to live—a place that reflects our values.

I've got big goals for what software can do for us in the future. I want it to change our lives.

It's already saving time and work.

But there's a lot more that software can do.

Today, many jobs involve using information. And this is one of the fastest growing job categories. But the problem is that information workers spend far too much energy doing dog work. They copy from one page to another. They translate information from one system to another.

Too often, they're doing the equivalent of moving hillsides with shovels and wheelbarrows.

Well, software can be our bulldozer.

In the industrial revolution, steam power and electricity freed millions of people from mindless physical labor. Now, better, more powerful software is going to free us from repetitive, unrewarding mental work.

Here's the good part.

Reducing drudgery creates opportunities.

Opportunities for people to be more creative in their work lives. To look for the next answer. To be more connected to others. And to realize their own hopes and ambitions through their work.

Not a bad goal for a few floppy disks.

Cyberspace is a new and sometimes puzzling place. It's a new social space—with new kinds of behavior. Some of it is straight out of the Wild West.

Computer technology has enormous power to make our work easier, our leisure more interesting and our lives richer. And the innovation and vitality of cyberculture will puts its own stamp on our larger culture.

But it's not immune to the rules of the road. It will prosper as it matures—and takes on responsibilities. In the process, the online world will take on the enduring values of our society.

We all have our part to do in taming this new land. Let's start by not stealing software.

Thank you.