

**EXPLORING  
CURRENT  
ISSUES & EVENTS  
IN CORPORATE  
COMMUNICATIONS  
2006 PAGE ONE TELECONFERENCE JOURNAL**

*Arthur W. Page*

ARTHUR W. PAGE SOCIETY

Arthur W. Page

ARTHUR W. PAGE SOCIETY

## VISION

The Arthur W. Page Society is committed to the belief that public relations as a function of executive management is central to the success of the corporation. The membership of the Society will embrace those individuals who epitomize the highest standards of public relations practice, as exemplified by the Page Principles.

## MISSION

To strengthen the management policy role of the corporate public relations officer by providing a continuous learning forum and by emphasizing the highest professional standards.

# CONTENTS • 2006 PAGE ONE TELECONFERENCE JOURNAL

---

- 2 Introduction to Page One Teleconferences:  
A Continuous Learning Opportunity
- 3 Avian Flu Pandemic: Perspective on Preparedness  
May 23, 2006
- 17 Privacy Matters: Safeguarding Identity, Data,  
and the Corporate Reputation  
August 22, 2006
- 31 Are We Our Vendors Keeper?  
November 1, 2006
- 47 2006 Officers, Trustees & Staff
- 48 2006 Committees & Task Forces
- 50 2006 Sponsors
- 52 Page Philosophy & Page Principles



ARTHUR W. PAGE SOCIETY

## **INTRODUCTION TO PAGE ONE TELECONFERENCES: A CONTINUOUS LEARNING OPPORTUNITY**

The Arthur W. Page Society's Page One Teleconferences were created to supplement the extended dialogue that takes place at the Page Society's Annual Conference, Spring Seminar and regional networking events throughout the year. These teleconferences are intended to provide fast, easy and timely discussion forums on subjects of current interest. They feature a moderator and guest experts who provide background, insights and advice about how corporate communications can help deal with changed circumstances in what are usually highly charged environments. The audience enters into a two-way dialogue with the panel and moderator. The transcripts of the Page One Teleconferences that appear in this Journal reflect the events and issues that have taken center-stage in public relations, corporate communications - and in some cases with people all over the world.

Please visit our web site at [www.awpagesociety.com](http://www.awpagesociety.com) to view or download the presentation materials mentioned in the transcripts.



## AVIAN FLU PANDEMIC: PERSPECTIVE ON PREPAREDNESS MAY 23, 2006

### PAGE ONE PANELISTS:

**Dr. Elizabeth McClure, M.D., M.P.H.**

University of Minnesota

**Cheryl (Cheri) Falvey**

Akin Gump Strauss Hauer & Feld LLP

**Jo-Anne Polak**

Hill and Knowlton Canada

**Moderator:**

**Thomas J. Kowaleski**

OPERATOR (TIM): Welcome to today's Arthur W. Page Society teleconference call, which is entitled "Avian Flu Pandemic: Perspective on Preparedness". During the presentation, all lines will be in a listen only mode. A question and answer session will follow the presentation and instructions for asking questions will be given at that time. Thank you for your attention, I would now like to turn the conference over to your host, Tom Kowaleski.

TOM: Thank you Tim, and good afternoon or good morning everyone. Thanks for joining us on the first of four Arthur Page Society Page One Teleconferences we're going to hold this year. Before we get into the teleconference, I'd like to open up the floor very quickly for a word of welcome from our President, Roger Bolton. Roger, it's all yours.

ROGER: Thank you, Tom. I just wanted to have the opportunity to welcome everyone and make the quick comment that one of the most important benefits of membership in the Page Society is the continuous learning opportunity. And we have found that the Page One teleconferences provide an opportunity to do this on emerging topics of current interest, and we certainly have one of those today. And I also wanted to thank

Tom Kowaleski, who recently retired from the senior communications post at General Motors, for taking on the leadership around the Page One teleconferences. Tom has brought a great deal of new energy to this and I'm really looking forward to our discussion today and the other great topics that Tom has planned for the rest of the year. Thank you Tom.

TOM: You're welcome, Roger. Let's get started. First of all, just to echo a little bit of what Roger said, we're positioning these teleconferences to be helpful door-openers to important and timely subjects that require the attention and involvement of communicators such as yourselves. Now, we have limited time -- just one hour -- so we don't pretend to make any of you experts by the time the hour is over. Rather, we hopefully will provide a good understanding of the scope of a major issue and provide some more detailed information on one or two critical areas of importance, and of course one or two major communications implications, learnings or helpful hints for you as you do your own investigations. We hope today will be a good example of that.

Briefly, let me tell you how the procedure will work today. We're going to have three short presentations by our panel of experts. I'm going to introduce them to you in just one minute. You'll hear all of their presentations uninterrupted. We plan then to have a good 15 to 20 minutes following their three presentations for your questions and their answers. The format for asking questions is rather simple, we'll explain that to you at the end of the presentation and we'll get right to it.

Let me introduce our three speakers in the order of their presentation. First of all, we're delighted to have with us today Dr. Elizabeth McClure. Dr. McClure is a Master of Public Health from the University of Minnesota. She is an expert on the origin and spread of infectious diseases and is knowledgeable in emergency preparedness and

policy issues stemming from these diseases. Dr. McClure is also the director for the Office of Emergency Response for the University of Minnesota, as well as a research associate at the Center for Infectious Disease Research and Policy. Her areas of interest include influenza vaccination, public health emergency preparedness, and policy development.

Our second speaker is Cheryl Falvey, and Cheri is a partner of Akin, Gump, Strauss, Hauer and Feld of Washington D.C. Cheri counsels clients on risk assessment in the major elements that need to be considered for excellent preparedness. Cheri concentrates her practice in the areas of product liability, in business court cases, and also in developing scientific presentations to courts and juries on these complex issues.

*"Seasonal influenza is a respiratory disease. It affects about one in five of us each winter, kills about 36,000, and hospitalizes a couple hundred-thousand more."*

- Dr. Elizabeth McClure

Our third speaker is Jo-Anne Polak from Hill and Knowlton in Canada. Jo-Anne has a very diverse background in media in government, in corporate and also in agency. She's a Senior Vice President for Hill and Knowlton, and is the National Practice Director of the Canadian Crisis Communication Team there. As might be expected, Jo-Anne has great expertise in the area of risk management and crisis communication. Jo-Anne also played a very integral role in the communication effort surrounding the SARS outbreak in Toronto, working with several levels of government, as well as several corporate organizations.

So we have three great speakers today. We're going to get right to it and then be ready for your questions and answers following that. I'm going to turn the conference over to Dr. McClure.

McCLURE: Thank you very much Tom. I'm really happy to be here. I'm most excited to hear the subsequent two speakers. I think I'm going to learn a lot, so I'm really happy to be included. Tom asked me to give you an overview of pandemic influenza so that we have a context for which then we can discuss some preparedness issues.

I did submit some slides, which you should have gotten yesterday, and what I'll do is simply say, "next slide" as I'm moving along. If you don't happen to have those slides loaded, don't worry. They're largely illustrations and I'll speak as if you're not seeing them. So, right now you should be seeing a title slide with my name and I'm just going to go ahead and say, next slide.

What I'd like to start with is to say that seasonal influenza and pandemic influenza are related to each other. In fact, as we have intermittent pandemic influenza outbreaks in our world, they really become the seasonal influenza outbreaks that we see then in the future. Seasonal influenza is a respiratory disease. It affects about one in five of us each winter, kills about 36,000, and hospitalizes a couple hundred-thousand more. It is vaccine preventable. Unfortunately, because the virus tends to modify itself -- or the family of viruses modify themselves little by little -- we require a new shot each year. Unfortunately, we haven't created much demand for influenza vaccine. Less than 30% of us in general get a flu shot each year. And so we really are behind the eight-ball in terms of our vaccine production strategies, and we're largely using a production system that was developed in the 1950s. Now, as we face the specter of another pandemic, we are hoping to improve quite rapidly our vaccine production. Next slide.

So what creates a pandemic? With regard to an influenza pandemic, the first thing we say is that we have to have a novel or a brand new virus. Now I can't really get into the nomenclature in ten minutes; but I'll just tell you that each year with seasonal flu, we tend to see the same H-sub

and N-sub types. So H1N1 or H3N2, H5N1 is a brand new type of virus that nobody has even partial immunity to, so that's one criteria for creating an influenza pandemic. Secondly, the virus needs to cause a serious disease, and we certainly have seen that with the high mortality rate so far for people who have gotten avian influenza or the H5N1 type. And lastly, it must be transmitted easily person-to-person. That's the last criteria that has not been fulfilled so far. Next slide, please.

We've had three pandemics in our last century. The misnamed, but very severe, pandemic of 1918 called the Spanish Flu killed between 50 or 100 million people, depending on who you read. There were two subsequent pandemics, however: one in 1957 and one in 1969. These pandemics were identified as such even though the mortality rate was much lower, because they were novel influenza virus strains -- brand new strains that we had never seen before. And so as I mentioned earlier, our seasonal influenza strains are pandemic strains of years past. So when you get a flu shot each year, one component of that flu shot is an H1N1 virus vaccine, and that is a remnant of the Spanish flu pandemic, for example. Next slide.

The natural reservoir for influenza virus in the world is in wild migratory fowl, and all human influenza virus arises from avian influenza viruses. Most of the time, migratory birds aren't symptomatic at all with influenza virus. They simply excrete it, and then it becomes an illness -- usually in domestic poultry -- and it can cause either a very mild illness or a very severe illness like we're seeing with the H5N1 subtype now. There are two ways humans can become sick. The first way is if a human being simply gets too close and has too much exposure to an avian influenza: to a sick chicken, or to poultry with an avian influenza. And that's really what we're seeing now in Asia and other parts of the world. The virus does not favor the human respiratory tract, but if you get close enough and enough inoculants, it can make you sick. The second thing that can happen is that the avian influenza virus can mutate in a variety of ways that I won't go into, so that all

of a sudden it does favor human respiratory mucosa, and when that happens then we start getting a preference of the virus for human beings. And that's when we start getting a rapid person-to-person transmission. Next slide.

This next slide really, I think, is redundant. As I mentioned, it is a disease of domestic poultry with an origin in migratory birds. We're looking at H5N1. We've seen a high mortality as it does affect human beings. Most importantly, however, is that we cannot really count on a seasonal respite. It's very tempting to say flu season is in the winter. What we learned from 1918 is that the first pandemic wave occurred in the spring. And so we can't take the summer off and think we're going to address this problem in the fall. Next slide.

*"The natural reservoir for influenza virus in the world is in wild migratory fowl, and all human influenza virus arises from avian influenza viruses."*

- Dr. Elizabeth McClure

It would be best if we could control this outbreak in birds. That's really the origin. And so here are some strategies that have occurred in Asia and other places in the world: vaccination of birds, looking for the disease through surveillance, culling of millions and millions of domestic poultry flocks and attempting to quarantine domestic poultry as well. Next slide.

The problems with this: number one, Asia is just simply too big. There are 13 billion chickens in China alone. Most chickens live in backyard flocks and in many areas of Asia there simply is no compensation for sick or dead animals, and asking people to cull or destroy their major protein source for the sake of the rest of the world is very difficult for people in that area of the world to agree to do. We currently see a reduction in poultry outbreaks in Vietnam and Thailand, and some people are saying, "oh, that's good news."

Maybe that implies that all of these control strategies are working. And I would have to say that I think that the way that influenza expresses itself in that environment is not well enough understood. And while I think we may celebrate that success, I certainly don't think that implies that we have this problem under control by any measure. Next slide please.

An example of that, I'll tell you how H5N1 started. Actually, H5N1 was first identified in human beings in 1997 in Hong Kong where it made 18 people sick and killed six of those. The Hong Kong government killed its entire domestic poultry population within three days and really made people feel that may have aborted a pandemic at that time. The virus seemed to disappear, and everyone thought well, culling all of those chickens was just the right thing to do and that influenza virus is gone. But in fact, that wasn't the case. In 2003 we began seeing it in domestic poultry in Vietnam in Thailand, and then it began affecting people in late 2003 and early 2004. Next slide please.

*"We know that we'll see a pandemic in the future. They just come periodically... We know susceptibility will be universal, but we don't know how severe the disease will be."*

- Dr. Elizabeth McClure

Currently, H5N1 has affected over 200 people in ten countries and several continents and killed 123. What has been sort of thematic about all of these infections is that they've occurred in non-industrialized areas, and in areas in which people live in very, very close proximity with their chickens. There has been a recent outbreak in Indonesia which appears to be potentially a family cluster. There's a larger concern there because the proximity to chickens cannot be as well described and because this family unit seems to be affected in such a way that there is a concern that there may be some human-to-human transmission going on. We've seen this in clusters in

the past. This has been the largest with the least association with domestic poultry. And so the World Health Organization may be coming out even today with a statement about the human-to-human transmission being seen in Indonesia.

So as we plan for this, we have to come up with some assumptions. We know that we'll see a pandemic in the future. They just come periodically. We don't know if it will be H5N1. I should tell you I've moved on to the next slide. We know susceptibility will be universal but we don't know how severe the disease will be. We really can just look at history to say that influenza generally has a short incubation period and what we know from pandemics in years past is that in general, pandemics come into communities in waves, last six to eight weeks approximately, with a peak of about two weeks, and that this could occur over 18 months to two years. Next slide.

The slide you should be on now, is a picture of the implementation plan from the federal government released in May. I apologize for the quickie remark, "don't worry we've got a plan" which is next to it, because this implementation plan is actually pretty good. One reason that I like it a lot is it does evoke sort of a yo-yo strategy that "you're on your own", but the truth is that the federal government cannot be the only answer for us. And I think even the plan itself it states that 85% of our critical infrastructure is housed in the private sector. And that's why it's imperative that communities, businesses and individuals undergo preparedness activities and not simply wait for the federal government to come up with a plan or a way to intervene on our behalf. Next slide.

It would be great if we had pharmaceutical infection control, but we really don't. We talked about the fact that our vaccine production is way out of date. The government is going to put some money toward that and there are some research efforts toward that which will improve. Our antivirals, as well, are not very good for flu. And again, we're trying to make more Tamiflu for example, every day. The World Health Organization is stockpiling Tamiflu. When

we do see a documented person-to-person transmission, they do plan to blanket that area with Tamiflu in an effort to reduce transmission. What we are left with is other non-pharmaceutical interventions called social distancing maneuvers such as closing school, keeping our children at home, preparing in advance in the workplace [by asking]: “how can you do some distance working?” and “how can you have non-punitive leave policies so that if people are sick they actually stay home?” We may be looking at some home isolation and quarantine and then efforts towards personal preparedness. We really have seen that if people don’t feel that their families are safe, they will not move to try to help the larger community. The next slide.

*“... it’s imperative that communities, businesses and individuals undergo preparedness activities and not simply wait for the federal government to come up with a plan or a way to intervene on our behalf.”*

- Dr. Elizabeth McClure

This slide should say “concerns” if you’re following along. Number one, in communities we must be ready to implement social distancing measures and we must have a reasonably high level of compliance for these to work. Number two, there’s a fundamental lack of traction for personal and community based preparedness efforts. We just can’t seem to get behind doing something when we don’t see the emergency right in front of us. And as communication experts, I think it is really an important goal to help people understand the necessity of preparing in advance.

The next slide says “Is there anything good about the bird flu scare?” and I sort of wish I hadn’t used the word “scare” but that’s okay. Number one, our vaccine production techniques will be modernized, there’s no doubt about that. Number two, we’re going to get better at looking for all sorts of diseases in animals and humans as

we improve our surveillance techniques. Number three, we are seeing, not just with pan flu but in general, a resurgence of public health. Back 30 or 40 years ago, public health really was eroding. Because of antibiotics and vaccines – especially with emerging infections diseases – we felt that we sort of had that licked. So not a lot of resources went into public health, and we’re seeing a reemergence, and I think that’s good. We’re going to see a modernization of our disaster communication system, and if we can get this part right, we can somehow encourage our citizens to be prepared for an all hazards approach to emergency preparedness.

The very last slide is simply a series of websites, and that concludes my comments. Thank you very much.

TOM: Dr. McClure thank you. Let’s move on to Cheri Falvey. Cheri?

CHERI: Hello everyone. I’m delighted to be here today to give you a lawyer’s insights into the pandemic planning process, and hopefully go over with you how to consider risks and identify the potential legal liabilities down the road as you start working on plans for corporate pandemic mitigation.

In talking about this, I think one of the dilemmas that we face is that pre-pandemic, one can seem somewhat alarmist, a “Chicken Little” type approach. And yet post-pandemic, we may look as though we didn’t do enough. And my perspective as a trial lawyer is interesting in that it’s usually a jury’s role to judge the reasonableness of corporate actions in hindsight. And so I wanted to start with that to give you a sense of my perspective, looking down the road, assuming a worst case scenario along the lines that Dr. McClure has laid out. How will your company’s communications and actions be judged? Were they reasonable? Did you do enough? And looking at this from the concern that pre-pandemic we may seem alarmist, let me first talk about the fact that it can be frustrating to feel as though you have

to try to immunize your company from liability for events that are somewhat out of your control. And yet, we know for a fact that influenza pandemics have occurred. We may not be able to predict when the next one will occur, but we know that they've happened over time. As Dr. McClure laid out, there was one in 1918 and smaller ones in '57 and again in '69. And so we have to assume that a risk exists and in these days where the media picks up on the risks and, in a very short period of time, has exploded the issue. If you do a Google search on avian flu or pandemic, thousands of information sites come up. And so now we have a risk that's foreseeable. And that's what, in thinking about legal liabilities, we look at.

*"... I think one of the dilemmas that we face is that pre-pandemic, one can seem somewhat alarmist, a "Chicken Little" type approach. And yet post-pandemic, we may look as though we didn't do enough."*

- Cheri Falvey

We look at "do we have a foreseeable risk, and if so what duties may exist that the corporation has to various constituencies?" And when you think about it that way, pretty immediately several constituencies jump to mind. You have obligations to employees, supply chain partners, customers, shareholders, directors, and officers. And it's thinking about each of those categories of duties that helps to put a finer legal point on this dilemma that we face between being overly alarmist at the start, and then post-pandemic, feeling that perhaps we didn't do enough. When I put a finer legal point on that dilemma, won't that depend on what lawsuit I'm looking at? Is it a claim that I've endangered an employee and failed to provide them with a safe workplace? Or is it a claim by a shareholder for liability for failure to have sufficient contingency plans in effect? Or for wasting corporate assets on plans that weren't viable and wouldn't have worked? Thinking about that latter point, how much money should be spent on

upgrading IT systems to enable workers to work from home if in fact an overtaxed system really couldn't support that in any event?

So those are the kinds of liability issues that, in just spending a few moments on this problem, jump to mind in thinking about how to handle the issue.

Let's turn then to what your key objective is in planning. One of those objectives is to make sure that you've identified the obligations you have to these various corporate constituencies, and make sure that you can demonstrate due diligence in managing those obligations and make sure that you can meet fiduciary duties to these various constituencies. You're balancing pandemic planning and investments that are prudent and necessary to protect the workforce against other risks that the corporation faces as well.

So what you're really looking for here is in hindsight: what evidence will I have that my corporation and its management, took safety seriously and committed the necessary resources, manpower and attention to the problem in light of how foreseeable it might be? And that's why it's so important to embrace accurate scientific information like the information that you've received today from Dr. McClure to help you categorize what the best approach is to the situation. You need to watch as the science emerges because it's changing almost daily in terms of the scope of this problem and we're obviously watching for that point when the virus can actually be transferred human to human.

To avoid the feeling that this is somewhat of a "Chicken Little" situation, many companies have realized that this pandemic planning is really just part of an overall corporate business continuity plan. Whether it's planning for hurricanes, a pandemic or a security risk more globally, these plans can be transferable between and among these various events. This helps you to mitigate against some concern that, "well, we don't know when this is going to happen, we don't know enough

about how it is going to happen.” And my thought on that point is that the implementation plan that Dr. McClure was discussing is posted now by the Executive Branch and is available on the Internet. That may turn out to be the standard-of-care on which your organization is ultimately judged down the road. And that’s why it’s so vital that you stay current on both the science and the resources available at the federal level for your planning purposes. In hindsight, someone’s going to look to see how your plans compare to the recommendations that were given at the federal, state and local level.

Now let’s talk for a minute specifically about some corporate communications issues that can arise. First of all, many times when policies are put into place regarding corporate compliance issues – whether those would be a sexual discrimination policy, or a pandemic planning policy – you have inter-corporate issues that arise. Dictating, for example, from a parent corporation how the planning process should work may lead to liability down the road if a sister corporation or a wholly owned subsidiary fails to follow through on the compliance recommendations. You can actually create more liability by mandating a pandemic influenza planning process if that planning process is not followed through at all levels of your organization. So one thing to look at is if we have built into this sufficient means of identifying whether the recommendations we’re making at the corporate level are actually being followed through by subsidiaries, by managers who are charged or tasked with certain activities. I’ll give you an example. The implementation plan has specific human resources tasks that should be engaged in reviews of available insurance, reviews of specific policies regarding sick leave, compliance with the federal statutes that govern labor relations. And if those recommendations are not followed through on, and it turns out that the recommendation to go forward and consider those policies is left undone, that can create liability. One way to deal with that is to provide suggested activities and disclaim the liability if that’s how your corporate structure is set up. Or you need to have built in to your planning process bench-

marks and timeframes for making sure that certain things are done so that you have the follow through on the plan to prevent that liability from coming up.

*“To avoid the feeling that this is somewhat of a ‘Chicken Little’ situation, many companies have realized that this pandemic planning is really just part of an overall corporate business continuity plan.”*

- Cheri Falvey

The other thing to take into account with regard to communication-specific issues is to go through – in thinking about your policies – what commitments and other statements you’ve made that, viewed through the pandemic lens, may not be statements that you can follow through on. So for example, if you’ve made statements on your website that say: “[insert your company name] is committed to doing business with suppliers who comply with local and other applicable LEVO requirements relating to health safety,” that statement may be fine in the abstract, but considered during a pandemic, that statement may create an implied warranty that you’re actually checking to ensure that your suppliers are in compliance with local health laws. And that may be something that’s impossible for you to do in a pandemic. So you need to look at your corporate communications to make sure that you don’t have any policies or commitments which are public in nature that may come back to haunt you in the event of a pandemic.

I think I’ll conclude my remarks there. I have a specific question that’s been raised by e-mail relating to sick leave policies. But why don’t I stop there and allow our other speakers to continue and then we’ll address the question at the question and answer period.

TOM: Cheri, thank you very much. And let’s now move on to Jo-Anne Polak, Jo-Anne?

JO-ANNE: Thank you very much. First I would like to thank you for the invitation today. I'm somewhat humbled to address this kind of an audience. And I certainly do understand that you are communications experts and for the most part crises communications experts. So I want to make sure I use the time that we have appropriately. What I'm not going to today is to provide communications solutions with regard to planning for a pandemic. That would be far too simplistic and arrogant. And I do understand that this is going to be different for everyone and every organization. But what I will do today is to share my experience with the 2003 SARS outbreak in Canada from a crisis communications point of view. I will tell you what I learned at that time, and what might be useful to you in your organizations as you go ahead with your planning process.

*"The public is going to be less forgiving with the avian flu, as the world really has had what they might consider to be plenty of warning and plenty of time to prepare."*

- Jo-Anne Polak

I, too, have a slide -- six slides. I'm still on the cover slide at this point. There are a couple of observations I'd like to make right at the beginning. First, given the fact that this is SARS in Canada, this is very much a Canadian perspective because that's the jurisdiction where my experience played out. So perhaps some of the findings that I have may be a little off, given the different regulatory and health care environments between Canada and the U.S., so I do want to make that very clear at the beginning. The second observation I think is important is that -- in Canada at least -- SARS came completely out of left field. There was little warning and little or no time to prepare, and that's not the case with the next pandemic. The public is going to be less forgiving with the avian flu, as the world really has had what they might consider to be plenty of warning and plenty of time to prepare. So because we were

so caught off guard with SARS, we probably were forgiven a little bit more for some of how slow we were to react. Next slide.

I'm going to talk a little bit about my SARS crisis credentials. As Tom mentioned earlier, we created SARS plans on the fly -- mind you -- for several corporate clients in Canada. We also worked with various levels of government on the SARS issues before, during, and after the outbreak. Just the issues, then the learnings around the government aspect of this are incredible and plentiful. There are all sorts of politics and it was a very complicated situation. We as a group all participated as delegates on April 30th and May 1st of 2003 at a national meeting where they brought all of the interested parties with regards to SARS -- the authorities and the experts -- together in Toronto to discuss this issue, and I was a delegate at that convention. But most importantly, out of all of the different SARS experience, I'm thinking the experience that would be most useful today, given the time that I have, is the insights learned from Hewlett Packard, HP. And I think out of all of the different learnings, the HP one was probably the most useful to me and I would think the most useful to you given the nature of the people who are on this call.

Just a bit of background: HP had one "probable case," which is where they believe that the individual probably does have SARS, and one "suspect case". Both of those cases were located in their Markham facility which is staffed with about 200 people. The Markham facility, for those of you who don't know, is immediately north of Toronto. The reason this was significant is because HP was the first corporate case of a "probable" and a "suspect" case outside of the hospital system. So as a result, it became very newsworthy. HP and SARS were headline news right across the country. And I have received permission from HP to discuss their circumstances with you today.

So I'm going to move to the third slide. The third slide is a picture of an iceberg. And so before I get into HP's response, I think it's important to share

with you their perspective on crisis communications that existed prior to the SARS outbreak. The iceberg really reflects the nature of what they believed was the effort required to fight any kind of crisis. The company believed that crisis is so much more than media relations. They believed at the time that using existing channels to deliver messages directly to stakeholders supplemented delivering them solely through a filtered media. They didn't believe in conducting less [media] relations, but they just believed that stakeholder communications was important. And I have to say that this stakeholder communications philosophy served them very, very well during SARS.

A little bit more background on HP and SARS: HP's handling of SARS is now considered best practice and the reason being -- again further to the perspective of after-the-fact -- is that through their stakeholder communications, they were able to immediately contain the disease. And that was extremely important. They used stakeholder communications to contain the disease. This was due to the fact that they were immediately able to communicate with all employees who had been in contact with the individuals and therefore exposed to the disease. Now the good news here is that the Markham site was a secure facility, so it was very restricted in terms of the number of people who could come and go. So it wasn't like a grocery store or something that had major impact on a lot of other audiences. The difficult side of that, though, is that we were very limited in terms of how much could be disclosed about that facility given the nature of the work. But HP was able to effectively impose home quarantine for all exposed employees and the disease was contained.

Now if you could move to slide four, "Strategic Considerations for SARS." The first learning -- and this is probably something a little odd for us corporate communications types -- but the one thing that was learned is that there were no circumstances where media coverage of this was a good thing for HP. Again this was [learned] after the fact, but media coverage didn't do anything to serve to contain the disease, but it did serve to create incredible anxiety among critical audiences

in all markets. Any time HP and SARS were mentioned in the same story, regardless of the context, people panicked. Rational people panicked. HP's employees were immediately shunned by their broad customer base, not just in Markham but all across the country. People were afraid that if they met an HP employee that they were going to be contaminated. Some anecdotes: there were sales people who would be delivering, for example, printer cartridges at an office manufacturing or retail front, and they would be turned away at the doors. Meetings were cancelled by customers across the company. And one woman -- I remember this story quite well -- was scheduled to help her mother move on a weekend and her mother called her and asked her to stay away.

So the impact on the company was not the impact they thought was going to come. The company ground to a halt because there were so many people who were concerned about being contaminated. So therefore, the company now did cooperate with the media and did deliver messages, but the company did not seek out media. HP was not, and this is extremely important, in a position to definitively declare that the situation had been contained. Even though they believed it had, there was always the risk that future contamination could be tied back to HP, and if this happened and the company had previously stated that they had contained the disease, the credibility with the public and the media would be severely damaged. And we saw this actually [happen to] the City of Toronto.

The City of Toronto was so eager to try to declare that it was a SARS free community -- because of the harsh economic impact -- that when SARS did return, it was more devastating than the first wave.

The second observation is that the balance between containment and sensitivity from a communications point of view is extremely difficult because they realized that they had to provide some kind of a balance between being sensitive to the poor victims who really were facing a deadly disease, and the fact they had to contain it. And they had to take a hard line with the employees;

they forced them to stay away while trying to provide the support that any employee who is through something so traumatic requires. So the right thing to do is obvious, but the action did appear harsh.

A third and very important observation in terms of SARS in Canada is that the companies and the corporations were not in charge. HP was not in charge. Our District Health Authorities were in charge. And you can actually leverage that and defer to kind of a higher power so to speak. While yes, you will have an obligation, a lot of the decision making power will be dictated to you by others. You're not necessarily the ones who will determine the course of action as it pertains to public health. In Canada, most certainly, that will be dictated to you by the local health authorities. Now HP had created and maintained a relationship with the appropriate District Health Authorities and respectfully and completely took direction as it pertained to this disease and this outbreak. And it was actually a very good thing, and HP was able to leverage it. So because HP or any other company is not necessarily credible when it comes to evaluating what is best for the public health, regardless of how much integrity a company has, the public may have a difficult time [believing] that the company's motivation is anything other than commercial. But the health authorities do have that credibility. And the foundation of all HP's messages throughout the entire situation was full cooperation with the health officials. They couldn't say that too much.

A fourth observation is what you say about yourself under these circumstances in terms of public dialogue is frankly irrelevant when compared to what others are saying about you, specifically your employees and your health authorities. HP was seen as being successful not because HP said they were successful, but because the employees and the health authorities really believed that the actions of the company was exemplary. And HP could have issued countless statements and taken credit but under these circumstances, being recognized by others made the difference. Now the flip side of that is also true. If the health authori-

ties single you out as behaving inappropriately, you risk being cast as the villain.

And the next point, number five, is that there is a very slim line in the public consciousness between a victim and a villain. This pandemic is no one's fault, but a victim basically is a company that takes every precaution to protect the health and well being of employees, customers, and suppliers – or seems to. A villain is seen as having spread the disease as a result of negligence in ability to identify those exposed and implement voluntary quarantine immediately. That was what we learned in terms of HP.

*"[During a pandemic,] a lot of the decision making power will be dictated to you by others. You're not necessarily the ones who will determine the course of action as it pertains to public health."*

- Jo-Anne Polak

The other thing, and to that end, point number six, is your objectives have got to be viewed as very highly principled and very transparent. So it's really all about containing the disease. Frankly, the worse-case scenario is not necessarily ceasing operation. The worst-case scenario would be if something you were seen to do – or not do – results in the number of cases going from 50 to 500. That's really what you're up against.

So the primary objective has always got to be to protect health and well-being. The secondary objective is the business contingency and corporate reputation.

The other observation that I have now in the three years since SARS is that I see a very dramatically different communications environment and media environment since SARS. Three years' [time] has been incredible in terms of the dissemination of information. It has changed. And while it didn't seem so at the time, at HP and HK, we had lots of time to discuss how to proceed and

craft messages accordingly, and we were able to get the stakeholders before they heard stories through the media for the most part. But that's not the case anymore and we all know it. Blogs and immediate electronic delivery of news and frankly, an ever eroding relevance of traditional legacy media is going to make communications during a pandemic more challenging than SARS every was.

In summary, my last slide is, and I think this goes to the last speaker, is: Don't just look to a SARS or other health related learnings as sources for learning. Look to Katrina. I think you can learn an awful lot from Katrina in terms of the impact at having multi-jurisdictions and the effective real time media. Look to the major blackout that happened in the Northeast and in Ontario in terms of operational disruption and how devastating it really is. And then finally look at the Faygo mining disaster in terms of the hunger for real time information and how quickly it can backfire. Thank you very much, and I really do appreciate having had the time to speak to you.

*"... the primary objective has always got to be to protect health and well-being. The secondary objective is the business continuity and corporate reputation."*

- Jo-Anne Polak

TOM: Jo-Anne, thank you very much. Cheri and Dr. McClure, thank you all very much as well. Let's go to some Q&A now, and I'm going to ask [the operator] if he will give us the method and the process of how you can all ask your questions. Before Tim starts, I would like to ask you all, though, to be succinct with your questions. If we can get through the questions and answers quickly, we'll also even provide opportunity to ask a follow up question then. So Tim if you'll take us through the process.

OPERATOR: Thank you Tom. At this time we will begin the question and answer session. To

ask a question please press zero followed by a one on your touchtone phone. Questions will be answered in the order they are received. If you have a question, please press zero followed by a one, now.

TOM: Okay, so we're all set. And Tim let us know if there are any questions that are coming in. I'm going to go to the question here that was sent to [Cheri] in advance, and it comes from Chris McQuen of Qwest. And Chris's question was on mandatory sick leave, that if an employee continues to show up at work with potential signs of an illness during a pandemic, and other employees are concerned, can we make the potentially ill employee go home? And what if they don't have any sick leave left? And are we required to pay them if we have to have them go home? So obviously some legal implications here. Cheri, would you like to take that one?

CHERI: Sure, I'd be happy to. And that is a very complicated question that we could spend a lot of time on, so let me try to simplify it and give a preliminary answer. The major recommendation that everyone is coming out with is to make sure that your sick leave and your medical leave policies don't discourage workers from staying home when they're sick or contagious. And what your question focuses on is the tension between your obligation under OSHA, the Occupational Safety and Health Act, to provide a safe workplace, free from contamination and other more general leave and labor policies. Frankly, the Fair Labor Standards Act, which at the federal level governs this, doesn't necessarily require payment for time that's not worked, whether that's vacation, sick days or holidays. But most employers in this country provide those benefits as a matter of agreement between the employer and the employee. And that can be even more complicated when you get into a union environment. The only real obligation is to maintain workers compensation insurance. On top of that is the Family Medical Leave Act, which requires certain employers who have employed more than 50 people over a certain very-specified period of time, to provide 12-weeks of unpaid, job protected

leave for family and medical reasons. And there are ways to document what the act governs.

So the sum and substance is that yes, if an employee is sick and you need to protect the workplace and the issues relating to that sickness – symptoms is probably the better word – to make you believe that it is an avian flu specific illness, then you can keep that employee away from the workplace and potentially they may not be paid for that. But you have to go over what your agreements are with the employees to figure out whether that really works in your individual circumstance. And if you need to revise those, you need to have a definition of a pandemic specific policy and, how that would trigger. Whether you want to tie that to a W.H.O. pronouncement or a U.S. government determination or a state determination, you need to have a very clear way of knowing when those policies will trigger.

TOM: Okay, thank you. Tim, any questions from the line?

OPERATOR: Yes, we currently have two questions in queue, and the first one comes from Peter Hurst. Please go ahead with your question.

PETER: Yes, thanks very much for a very interesting presentation from all of you. I do have a question for Cheri, which relates somewhat to the previous question as to whether there's any kind of bright line between the preventative steps that a company might take towards its employees and what it would not reasonably be expected to do. I'm thinking in terms of a company with 120,000 employees providing Tamiflu doses to its entire workforce. Would that be a reasonable expectation?

CHERI: Well, as you know, it's a very moving target. It's whether that's reasonable given your financial situation and the other things that you need to plan for, document, etc. It is very individualized. You need to think of it this way, if it doesn't make sense for your company to assume that

kind of a financial obligation, then how would you have gone about thinking about that and making the decision that its not the right thing for your company to do? And you'd want to document that you considered it in light of the fact that some companies are indicating that, to the extent that they can obtain it, they'll buy it. I think it will be interesting to hear from Dr. McClure about whether that's really going to work and how much will really be available. The same would go for vaccines and the fact that you don't want to get out there and commit to something that you can't fulfill. There may not be vaccine available. So from a liability perspective, you need to have thought about all that and if you make a decision one way or the other, you need to document why you've done that.

*"The major recommendation that everyone is coming out with is to make sure that your sick leave and your medical leave policies don't discourage workers from staying home when they're sick or contagious."*

- Cheri Falvey

PETER: Thank you, Cheri.

TOM: Dr. McClure, would you like to comment on anything in terms of the availability and some of the points that Cheri raised?

MCCLURE: One thing that I know officials are really trying to discourage is any sort of personal stockpiling of Tamiflu. Most certainly it decreases our ability to use Tamiflu effectively. The World Health Organization is attempting -- as one of its strategies -- to blanket a particular small geographic area with Tamiflu, should there be some kind of sustained person-to-person transmission documented. The concern, of course, is that people will stockpile Tamiflu and take it inappropriately and at the wrong time and simply dilute resources that we otherwise would need.

The second piece is that we don't have a pandemic virus that exists yet and it's unclear which type of antiviral will be most effective. If I were a company -- and this isn't my area of expertise -- but I would not invest a lot of money in something that is not clearly going to be effective.

TOM: Okay. Let's go to another question.

OPERATOR: Thank you. And as a reminder, if you'd like to ask a question, you may do so by pressing zero followed by a one on your touch-tone phone. And the final question in queue comes from Cam McCullis from Carleson Company. Go ahead with your question.

CAM: Yeah, this question is for Jo-Anne. Jo-Anne, what would you consider to be your top six elements of a basic communication plan?

JO-ANNE: I'll give you some of the top elements. I think the first element is to have a really good handle on who your stakeholders are and how you would reach them in terms of not just a pandemic, but in terms of any crisis. Who would be the individuals who would be in touch, who would be responsible for reaching them and how you would be able to reach them if for some reason you were off site? So I think that's extremely important -- the stakeholder communications.

Secondly is to identify the different health authorities that you can defer to over the course of between now and when and if anything ever does break out. Get a really good understanding of the different levels of government and perhaps even begin to open some kind dialogue with them. Because I think that would be able to help you should a pandemic hit and these people all of a sudden become very busy. The fact that they would have had a pre-existing relationship with you, I think, would be extremely important.

I think the other thing that's important is to clearly communicate the policies in advance with your employees so it doesn't look as though you're making it up on the fly when and if something does hit. So if you can always say as "we discussed

earlier, this is the course of action that we're going to take," I think that's extremely important. But I think we have to rely less on the traditional media relations. And I think we have to really beef up our stakeholder communications and employ things such as telephone trees, for example, if we have to speak to customers. HP used telephone trees for executive outreach to try to dispel this information and so forth. So I think it's having the direct channels in place so that regardless of whether it's this or any other kind of a crisis, you're able to deliver your messages directly to those audiences.

I think another thing that's interesting is that the people who tend to populate the blogs and the internet chat and so forth, also tend to be people who have a relationship with your stakeholders. So the more dialogue you have with the stakeholders, the more the stakeholders are then going to feed that dialogue back through the blogs. Not that you necessarily want that, but that's what's going to happen, and also through the media.

TOM: Okay, thank you. Tim, any other questions?

OPERATOR: There are no further questions at this time.

TOM: Okay, let me throw one in here. I will open this to our three panelists. A couple of days ago, the Wall Street Journal ran a piece that talked about the World Health Organization endorsing the use of older antivirus drugs, such as Amantadine and Ramantadine, in addition to Tamiflu, which Dr. McClure talked about. It seems the way the story positioned it, that this was an answer to a concern over the scarcity of supply -- or the potential scarcity of supply -- of Tamiflu. First of all, Dr. McClure, is this something else that you think will be a satisfactory answer in that area? And then secondly, Cheri, do you see any potential legal aspects that may stem from having a choice of different kinds of antivirus medicines to choose from, i.e., could one work better than another? Therefore, does that set up some legal precedent as well?

MCCLURE: I can just speak briefly to the study. A group of researchers went back and looked at over 600 avian influenza viruses that have been collected from several Asian countries and when they looked at those with regard to their response to antivirals, they found a little bit surprisingly that they were more responsive to, what we would call, older but still commonly used antiviral agents. Being older shouldn't imply they aren't in production anymore. We use them every year for seasonal influenza. They just aren't the latest antiviral that has been developed. Early on in the outbreak, the initial assumption was "oh, these aren't very effective and we're going to need to go to our newer generation, the Tamiflu type of antiviral." But in fact, they went back and tested all these samples and said no, that actually they may have a greater susceptibility than we thought and perhaps using several antivirals in combination may be the best bet of all.

And again what people are trying to do is get clues from the existing avian influenza virus so that when a pandemic influenza viral strain occurs, if this H5N1 should mutate to be able to spread person-to-person, it will also have a different response to antivirals. To continue to, sort of, put a face on this and get a sense of what this virus might do is important. So that was what this study is about.

TOM: Cheri, we have just about 20 seconds, is there anything you'd want to add from a legal standpoint?

CHERI: I guess just to caution that this is an area that's fraught with legal concern. There are reports from Japan back in November of 2005 about childhood death from the use of Tamiflu, and some other neuropsychiatric events. And going back to the Swine flu, there were issues relating to vaccines causing harm when the threat was "overrated". So, I would put some of the other protection activities -- even things as simple as washing your hands and social distancing -- as a higher priority than the use of these other, the antivirals.

TOM: Okay, thank you very much. And that's going to conclude our time together here this afternoon. First of all I want to thank all three participants, Dr. McClure, Cheri, and Jo-Anne. Really excellent presentations. Thank you very much. Very succinct, got a lot of information out. We're going to make a transcript available to everybody who was on the call with us today. I'd like to also solicit your thoughts on this format, how we might better attune it to your needs and desires in the future, as we look at doing three more of these before the end of the year. And if you have any ideas in terms of next topics, please get them to us, and you can send those to Paul Basista at Arthur Page, and Paul's email is [exec@awpagesociety.com](mailto:exec@awpagesociety.com).

*"I think the other thing that's important is to clearly communicate the policies in advance with your employees so it doesn't look as though you're making it up on the fly when and if something does hit."*

- Jo-Anne Polak

I would like to thank Paul Basista and Susan Chin from the Page Society for putting together all the details of this conference and making sure it ran so smoothly, and also I want to thank Roger Bolton for his continual support of doing this on behalf of the Arthur W. Page Society. And we look forward to being in touch with you for the next one and doing three more of these this year. So thanks very much. We really appreciate you joining us all today. Thank you.

OPERATOR: Thank you all for your attention. This concludes today's conference call. All participants may now disconnect.



ARTHUR W. PAGE SOCIETY

## **PRIVACY MATTERS: SAFEGUARDING IDENTITY, DATA, AND THE CORPORATE REPUTATION**

### **AUGUST 22, 2006**

#### **PAGE ONE PANELISTS:**

**Harriet Pearson**

IBM

**Fred Laberge**

Aetna

**Toni Simonetti**

GMAC

**Moderator:**

**Tom Kowaleski**

TOM: Welcome to our second Page One Teleconference of the year, called "Privacy Matters: Safeguarding Identity, Data, and the Corporate Reputation." This is Tom Kowaleski, and I'm pleased to be the moderator for this one-hour session offered by the Arthur W. Page Society.

First of all, I'd like to say that our Page Society President, Roger Bolton, could not be with us today but sends his regards and thanks to all of you for your participation. Before starting today, I just want to say a couple words on the procedures for those of you who may be attending one of these teleconferences for the first time. This the second of four teleconferences we're going to do this year. Our intent with these conferences is to provide a snapshot of some of the most important issues facing the communications profession today. Admittedly, these will not make anybody an expert, but rather, will hopefully open a few doors of learning and provide an excellent foundation for you in your own work and further investigation into these critical areas. These conferences are designed for your participation, so we encourage you to take notes and jot down questions as you listen to our three expert speakers this after-

noon. At the end of the speakers, we expect to have a good 15 or 20 minutes of Q&A time. While you're on the line now, your phones will not be connected in two-way conversations. I know a number of you are in conference rooms today, so you can speak with each other and I will alert you when it comes time to open the Q&A.

I will remind our speakers, though, that your phones are open for two-way conversation, so if you want to make another comment to any one of your colleagues who are speaking today, you're going to be able to do that.

This is how our Q&A session will work this afternoon. To ask a question when we're ready, you merely press zero then one and, the conference operator will come online. She will ask your name, your affiliation and then tell you when you are in live with the conference and then you can ask your question. State your name and affiliation and then direct your question to one of our participants. Please try to be brief and succinct so that we have plenty of time to get all the questions in.

We have sent out a small package of slides. These slides will give you some background on what our speakers talk about this afternoon, and they will track the subject of each one of their presentations, but won't be exact. So I remind you to use these only as a guide. They will give you a good idea of their topic, but also please listen closely as well because there will be a lot of new information that each of our speakers is going to discuss this afternoon.

Again, our topic is Privacy Matters: Safeguarding Data, Identity, and the Corporate Reputation. This is literally a subject that involves every company today. Seemingly not a day goes by without us seeing and reading a media account about increasing privacy policies and practices, breaches

in any one of a variety of ways -- from hacking to physical property theft. This has major employee communication implications as well, ranging from communicating the proper and adequate preventative policies and actions, to sensitively and clearly communicating necessary information, new requirements and needs following a breach. It's a global issue, as regulations and privacy practices vary from region to region and country to country and, as we all know, this often challenges and affects a company's desire to have one policy and process to cover their world operations and world needs. More than likely, both the preventative work and actions occurring after a breach involve more than one company. It can involve complete supply chains; it can involve government, and as we're going to hear this afternoon, perhaps involve multiple companies in the same industry. And it is getting increasingly all-pervasive in our daily lives. For example, both the New York Times and the Wall Street Journal today carried stories touching on the privacy concerns that will be emanating from a new regulation requiring automobiles to carry black box data recorders beginning in September of 2010. There are going to be a lot of privacy implications coming out of that.

So now to our speakers today. We're really lucky to have three outstanding experts and practitioners in this subject matter. First up with us this afternoon is Harriet Pearson. Harriet is the Chief Privacy Officer of IBM since November of 2000. In addition, she's also the Vice President of Corporate Affairs at IBM. She is responsible for guiding privacy policies and practices across the company, streamlining privacy initiatives within IBM business units and regions, and also furthering the efforts and knowledge the company uses itself and provides to service clients. Harriet has consistently been on the leading edge in developing these practices and processes.

Now, following Harriet's overview on this subject and the critical role communications and communicators play in it, we're going to have two speakers who have both been deeply involved in and successfully managed a wide array of communica-

tion issues resulting from privacy and identity breaches in their own organizations.

First is Fred Laberge, and he is the Assistant Vice President of Corporate Public Relations at Aetna. Fred is responsible for providing strategic communications counsel and media support to the CEO of the company, as well as the finance, legal, regulatory affairs, HR, and IT departments, and also a number of business units throughout the company. Aetna was recently involved with the Department of Defense laptop theft issue, and because of the government implications, this became a highly visible and much-covered event. Fred will take us through Aetna's communication strategy and actions and let us know the successful conclusion and some good practices that they have developed along the way.

Toni Simonetti is our third speaker today and she is the Chief Communications Officer of GMAC. For a number of years when we worked together, she was also the Executive Director of GM's Financial Communications, Media Relations, and Public Policy Communications. Having been at GM at the time of the identity theft incident that Toni's going to talk about this afternoon, I can vouch that she and her communications team were an integral part of identifying, strategizing, and then managing the multiple communication challenges resulting from it.

So we're going to ask that our three speakers do their presentations in order, and then we're going to open up the Q&A lines to you. So, Harriet, we're pleased and privileged to have you with us today and we're going to start with you.

HARRIET: Thank you, Tom. I'm happy to be here, enjoying such an august group. If you could turn to page two of the charts that I've sent out, I will start by framing the challenge facing us as corporate leaders, whether we're in communications or another group inside a company. And the challenge, I think, is a fairly broad one. Tom opened up with a very good framing, but I would just add to it that the simple choice between what most of us would want to call "private" or "not

private” is really becoming harder and harder to offer to our customers and other stakeholders. Even though the consumer desire would be to keep things private, these kinds of choices are no longer possible. Instead, I find myself and my colleagues who are privacy leaders in other companies, searching for new ways to meet the very human need to have a zone of privacy. This is true particularly in North America and Europe, and increasingly so in Asia. The knowledge that I have from consumer studies and other reports about what consumers are really looking for [says that consumers want] to trust that information about themselves is being managed well and that things are under control; that there’s a zone of private behavior that is available to them, but also the knowledge that if they do share their information, there is some trust that it will be managed well. And I think that’s what we need to focus on in our corporate communications, and in our corporate actions underlying those communications. And I think what’s at stake here is at the broadest level is corporate reputation, and also our ability as businesses to operate with a certain freedom of action and trust that we’re doing what we say we are doing.

I think that’s the challenge. And the key related developments that are affecting the landscape this year and which have implications beyond can be put into five categories. If you turn to slide three, I think the data and security breaches that have made news in multiple industries are clearly top of mind for many of us -- both the prevention of these data breaches and also what to do if you have one and have to report it. Why is this such an issue right now? Are we having more security breaches than we’ve had in the last decade or so? Arguably, I would say no, we’re not. I think all of us who are in the security field and know what the patterns of potential violations and violations have been for the last decade or so since the Internet emerged, have a feel for the fact that we’re not necessarily seeing more breaches, but we are definitely seeing more requirements to report incidents that may lead to compromise of data, starting several years ago with a law enacted in California -- the leading edge of so many differ-

ent public policies -- that actually requires notification. Now in the United States, approximately 39 States have these requirements. There’s Federal legislation pending that would require notification, and importantly, a couple of other countries have looked at what’s happened in the United States and are considering similar legislation. Canada, Japan, and Europe are all looking at this, and in Japan, in particular, this requirement is already there. So what’s that done? It made data risks evident to all of us -- all consumers and all of us. There is risk inherent to managing data.

*“[Consumers want] to trust that information about themselves is being managed well and that things are under control; that there’s a zone of private behavior that is available to them, but also the knowledge that if they do share their information, there is some trust that it will be managed well.”*

- Harriet Pearson

The second big trend that has implications for communications, certainly -- and for corporations ranging from Google to AOL to any of us who are involved in supporting government processes -- is private observation for public purposes. The slide should read, “Private observation for public purposes.” Increasingly, government is looking for access to information held by the private sector to achieve public ends, such as fighting terrorism, securing our airspace, helping the security of supply chains or other kinds of activities that are associated with public goods. Consider, if you will, the controversy over passenger records between the E.U. and the U.S. The U.S. would like more passenger information in order to secure our air space, and the E.U. is resisting handing over manifests of passenger information because of the privacy issue. How does one deal with that? How does one deal with the ramifications to clients, to investors? How do you communicate those issues?

Consider also access, by governments such as China, to information held by the private sector, and the controversies that have implicated some of the Internet service providers, for example, and other companies in emerging markets where these notions of privacy are, perhaps, different than what we have in North America and in Europe. Those are significant issues hitting multiple sectors.

*"Increasingly, government is looking for access to information held by the private sector to achieve public ends, such as fighting terrorism, securing our airspace, helping the security of supply chains or other kinds of activities that are associated with public goods."*

- Harriet Pearson

The third development that I think will be with us for quite some time is globalization. Globalization of business processes in particular – whether it's outsourcing of key processes or just locating functions in a more global basis with the resulting access to data that might be held in other countries – has implications. The European Union, as some of you may know, has had long-standing data protection or privacy rules dating back to the early '90s, which have been implemented now in all of the E.U. countries. You have 25 significant countries that have restrictions on whether data can be accessed – not even moved, but even accessed – by those outside of the E.U., as well as special requirements that have to be met, and concerns about access by non-E.U. citizens. These have significant implications for compliance within corporations, but also as conflicts arise, such as the ones between the E.U. and U.S. on passenger record data involving the airlines, you have communications challenges as well. The rise of Asia, in this context of globalization of business processes, is significant because with the rise of Asia – whether you're talking India, China, or the other markets there – privacy is not considered in the same way. India and China in particular have very different notions of privacy

and do not have uniform legislation on this such as Europe has. It's an issue to keep an eye on over time.

The fourth significant trend is the transformation of health care in the U.S., but also in multiple other markets. With the advent of electronic medical records and the increased use of the Internet to both collect and manage medical information on the back end but also, frankly, in the consumer context of having health care information available on the Internet to manage on the consumer end, and the web-based entrance in this market, privacy issues are raised which go beyond, for example, the U.S. federal health privacy law called HIPAA. So these issues go beyond HIPAA and it's an area of new policy making, new standard setting, and frankly, new communications that can be had with employees who are now accessing health information via web based personal records or other means.

Finally, wrapping up with the fifth privacy related developments and trends in this year and beyond, new technology such as RFID, Radio Frequency Identification Devices, and other new technologies can spark advocacy and legislative activity to either restrict the usage of these technologies or to regulate it. And this kind of cycle has always been with us as new technologies or new uses of technologies have come about, but this I think this couple of years have seen RFID pop out as one of those uses, or one of these technologies that captures the mind, captures the public advocacy, and there are a few others that we can get into if there's interest in the discussion.

So these trends – if you go to the next page – are not limited to North America or the United States, where most of this probably sits. Most of us probably have interest in international, if not global, business. I include this map to indicate that there are some areas of the world that have multiple kinds of these laws/legislation, or legislation that's pending, and this is an international set of issues and should be approached and managed as such, due to, of course, the fluid nature of information as well as communications.

If you go to the next page, I offer a point of view about how to ensure that your business is positioned to protect the corporate reputation and frankly, to protect your freedom of action to execute your business model. And I take this strategy of best practice from our own experiences at IBM, and also from what we've observed working with our clients and the multiple groups with which we are involved, in trying to set best practices in this day. So we've been at it for quite a while. I'll go to the next slide in a second that will talk a little bit about our length of history in this space. But I'd say very simply, at the highest level of the corporation, it's not a very difficult equation to solve to be sure that you are ready to minimize your risk and protect your reputation.

First of all, I'd say one needs to begin by understanding what the risks are and to invest in managing them. Risks are never going to be reduced to zero, particularly in the area of security breaches, but they can be reduced. And so first and foremost, I believe that the head of the corporation must have some organization for scanning how changes in business models and practices can change your risk. This should be on file. For example, if we have outsourcing, if we have a location of business practices moving from one region of the world to another, if we have new employees managing processes, how then are the risks to the data, which are under your control and management, going to change -- based on changes in your business? And importantly, I think security managers and corporate managers used to think only about risks to the corporation and risks to the data that were corporate data. So you had people managing intellectual property and protecting it. You had people managing financial information and protecting it. And you had people managing, let's say, customer information, protecting the mailing list or protecting the integrity of that, but not necessarily focusing on the risk to the individual whose records are in there. Well, I would say one of the key paradigm shifts we have observed in the last couple of years is that now we as corporate managers are going to be held accountable -- in the media at least -- for the risks to the individual whose information may or may not be com-

promised while under our stewardship. That increases, or at least changes, the privacy and security calculus.

So first, ask your corporation and your corporate colleagues how well are they assessing the risks and managing to them, so you know where your exposures are.

*"... we, as corporate managers, are going to be held accountable -- in the media at least -- for the risks to the individual whose information may or may not be compromised while under our stewardship."*

- Harriet Pearson

Second, prepare for the inevitable incidents. I kind of go to bed every night thinking, "Yeah all right, maybe tomorrow is the day for us." And we've had a few incidents. Thankfully we've managed through them pretty well, but it could happen to any company and even name brands have gone through incidents -- whether it's a stolen laptop that is not data encrypted -- or if it's something perhaps different in its configuration -- these things will happen. And ask your company, to drive the adoption of a security or privacy incident response plan if you don't have one. Know who is responsible for reporting; make sure your employees are educated; don't let the plan get out of date; and don't let an incident get out of your control by not having a process that shows that you are going to be responsive, that you're going to have all the data that you possibly can, that you have thought out who does what if something like this does happen. By the way, because your businesses are likely to be operating outside of the U.S., consider that the data which you may be responsible for notifying about may actually be outside the U.S. So extend your process to be outside of the U.S.

Third, confront any incidents or issues very quickly. I would say that ahead of whenever you have an incident is a good time to think about it

and actually get involved in industry groups to build best practices, or to minimize the risk of even a security incident happening within your own business or with your suppliers, etc. But be ready to be active in that way over a fairly extended period. Especially if you have an incident, you need to re-establish trust. And I mentioned just a few companies on these slides and these all have been in the media. The Veterans Administration, for sure, in the government context, has a long way to go to re-establish trust and how they manage security and privacy. Eli Lilly, years ago, had a famous case where they mailed out Prozac marketing to people who were taking or had taken Prozac, but they famously forgot to 'BBC' the distribution list in the email, and instead put it in the 'CC,' and thus compromised the identity of all of those folks. They have been executing under a consent order from the U.S. Federal Trade Commission now for some years, and have rebuilt trust, I would argue, but it's taken a while. And similar with other companies.

*"[Corporate managers need to] prepare for the inevitable incidents. I kind of go to bed every night thinking, "Yeah all right, maybe tomorrow is the day for us.""*

- Harriet Pearson

Final point here, so I can turn it over back to Tom, is that in my experience, communication plays a key, paramount role. And I don't say this just because I actually am part of our communications function here at IBM. Even before I joined our communications team, I was a strong partner with communications for the almost-10 years that I've had this responsibility at our company. It's communications on the internal side, to ensure that employees understand their obligations and responsibilities with respect to how they manage information and protect security. It's the executive communications, so that as company leaders go about their day-to-day activities, they have the key messages to drive their company forward. This kind of understanding is embedded in the

appropriate way in the highest level messaging and activities for the corporation. And finally, from an external perspective, not only having a media team that is available to help in assessing how to respond, but also how to be proactive. Where are the opportunities to take activities around security and privacy and leverage them for the benefit of a brand, or at least to understand how to behave and how to drive forward, consistent with our brand and our external relations strategy? So I'd say that it is fruitful for corporate communications to be partners with other functions in the company, and especially to tie it to these important trends of globalization and changes in business process and reputation management.

I'll conclude with just a couple of pages that are interesting to me. When I first started working on privacy at IBM, I saw that IBM had a long-standing history in this area, and was actually THE first corporation to develop a global privacy policy, back in the 1960s. That subsequently, and ultimately, became a basis for the OECD to develop some global guidelines for multi-national corporations. And I've been acting as the Chief Privacy Officer now for six years, and we were one of the first companies to appoint a senior person to oversee this, and we have made investments in research and privacy enabling technologies, not necessarily as money making opportunities, but as a strategy to make sure that we are enabling the other offerings that we've put into the market, with some syncing here that would be helpful for the long haul.

I have a couple of illustrations on page seven, of how, over a sustained period of time, our issue strategy -- if you'd want to call it that -- around privacy has been sustained. Over the last decade that I've been involved, we have maintained attention to this issue and have carefully worked on a few initiatives to ensure that we are able to stay on this leading edge. And we have been recognized for that, for which I'm very thankful. But on the last page, before I turn it back to Tom, there are a couple of resources for you if you're looking for best practices, or general references,

or just good people to talk to about these issues and how to manage for your own company. We can go into that if there's interest during the Q&A. Tom, I'll hand it back to you.

TOM: Okay, thanks so much Harriet. I think that last page will be helpful for a lot of people.

Let's turn our attention now to a couple of specific examples of very large companies who have faced some significant challenges, and a couple of instances here and how they successfully managed them. So we'll kick off here first with Fred Laberge from Aetna. Fred, it's all yours.

FRED: Thank you very much. As you said, I'd like to address this from the perspective of a company that's gone through an incident and thought about many of the things that Harriet mentioned in her comments. We had a real problem back in April and I'd like to talk about how we dealt with it. The slide deck that I put out, if you turn to page two, prefaces this a little bit by setting the scene to explain to you how we ultimately dealt with the D.O.D. incident that we were victimized by in April.

About a year ago, or maybe a little longer than that now, we had taken a good hard look at how we manage data and information privacy here at Aetna. We were very much aware that other companies, particularly some financial services companies, had had media related to incidents that occurred to them, and we were thinking very hard about how we might manage an incident like that ourselves. We already had a crisis event response team in place that was cross-functional, not just communications, but obviously the law department, investigative services, security, a whole range of areas within the company. And we have a privacy officer, but he dealt mainly with compliance issues since we're a very heavily regulated industry. The health care industry in this country is generally not federally governed, so different rules apply in many different states. In addition, the health insurance portability act, HIPAA, that Harriet mentioned, is something that our privacy office dealt with. And then of

course the whole IT part of the company was dealing with the data itself and how to secure it. We were very confident that we were pretty well protected against breaches from outside. Essentially we felt we had strong firewalls and we could prevent hackers and so on. What we were less confident about was what ultimately happened -- that a laptop gets stolen, or an employee steals information, or something like that. And what we set about doing -- back in January, our Board of Directors had become very interested in this -- was to set up a team to work on information privacy and to create a communications framework to help our employees begin to understand the need for information privacy security.

As Harriet also mentioned, we have a lot of health care information, PHI as we refer to it, Private Health Information, of our members. We have their social security numbers and a lot of other data like that. And we wanted to make sure that our employees understood the importance of protocols for dealing with this sort of information and that they understood the implications of a breach if something were to happen and how it could affect the reputation of the company. We would often report on incidents that occurred at other companies on our own company intranet, for example. Nonetheless, in April we had an employee in one of our field offices who had a laptop computer locked in her car. She had stopped on the way home from work at a convenience store to pick up a loaf of bread or something. And during the three or four minutes that she was in there, her car was broken into and the laptop was stolen. And as it turns out, even though we had gone through a number of communications and other compliance announcements saying that everyone who had a laptop should have it encrypted, she had not done so. It was on her list of things to do but she hadn't gotten around to it. And now we were in a real fix.

And we had to find out -- obviously -- what was on the laptop, and it turns out that she had the private health information of about 38,000 people at the Department of Defense, an Aetna

customer. We immediately notified the Department of Defense, obviously, and began to work with them to try to understand what was on the laptop. You should understand that these were not people who were generals of the armed forces; these were people who worked in PX's and places around the country that provided services to the armed forces. They were not military themselves, so there was not a chance that this was information that would be taken from somebody who worked in an intelligence operation or something like that. Nonetheless, we had to take it very seriously and the interesting thing was that we had to sort of take our direction from the customer -- in this case, the Department of Defense. The way our health business works, the customer is essentially a company like those that you represent. And our members are the employees of those companies. So we worked very closely with D.O.D. to help determine when and how we should communicate. Understand, again, also that there was never any indication that the information had been misused in any way, and there still isn't. Nonetheless, we determined that the responsible thing to do was to essentially "fess up." You have to come out and say that you've had an incident like this. You have to do the right thing and take all possible steps to make sure that the public understands. There are a number of laws -- it started in California -- there are laws in a number of states that require notification once an incident occurs, and we had to look at all of those and it was evident very quickly that we needed to put out a statement.

As often happens in corporations, timing can be quite unfortunate. This incident occurred within a day of our year-end earnings announcement, our fourth quarter and full year earnings announcement back in April, and the day before our annual shareholders meeting. And so we had to think about positioning this and how it would be received by Wall Street because the kind of reaction that you get is very scattered. And you can see this in the slide that I've got on the third page of the presentation. We essentially had wire service coverage -- you know ... AP, Bloomberg, Dow Jones, Reuters, etc. -- which was widely distrib-

uted, and yet we got various interpretations of the same basic information. Some of the coverage ended up being somewhat positive, and by that I mean that it really emphasized what the company was doing to remediate the situation. Other coverage was very negative and was focused on talking to impacted D.O.D. employees and others who said, "Oh my God, I feel so violated!" and that sort of thing. And then obviously the more objective, impartial statement of the facts. But I find it fascinating that we had such a wide range of coverage, in essence, emanating from the same few stories.

*"... we determined that the responsible thing to do was to essentially "fess up." You have to come out and say that you've had an incident like this. You have to do the right thing and take all possible steps to make sure that the public understands."*

- Fred Laberge

Another thing that I would add is that the coverage can be less than responsible. I don't want to say irresponsible, but for example, we had a typical news story on a TV station, I think it was in Detroit -- a Channel 4 Action News kind of story -- that essentially reported Aetna had had a computer stolen and if you are an Aetna member you should call the company right away because there's a chance that somebody's got your private health information. Now, we've got 14 and a half million members and we're talking about the potential for a handful among those, and they had to be employees of the Department of Defense. Yet we started getting phone calls from employees at General Motors and Ford and other large companies in the Detroit area. And so again, it's something for you to keep in mind that if something like this gets out, it's pretty hard to put the genie back in the bottle. You've really got a lot of work on your hands, and there's a lot that you have to do in communicating not just with the media but with your affected customers. In our case, in the health care industry, we have the

members, the individuals who have the health insurance policies, we have a broker sales force that sells these, so we have to get to our own sales force and then the brokers, we have the government relations implications, we have to notify the various states we deal with and especially given the timing, we had to deal with the investor community, the analysts and others, and this became kind of a side show to our earnings announce-

*"Some of the coverage ended up being somewhat positive... Other coverage was very negative and was focused on talking to impacted D.O.D. employees and others who said, 'Oh my God, I feel so violated' and that sort of thing."*

- Fred Laberge

ment. Then there's speculation if the stock moves up or down, and well, the stock moved down that day, and people would speculate that it was driven by this, rather than your financial results.

So again, you can see the potential impact of an incident like this on a company, even if you've taken steps to. And we had already, as I said, had in place for more than six months an employee education program with requirements for encrypting laptop computers and then desktop computers, putting cable locks on machines and we had a wide range of information security practices that we were working very hard to get into the culture of the company. Despite all of that work, one rogue employee who failed to follow instructions led to what turned out to be a long-simmering problem.

There are a couple more slides that I'd like to show you, if we can skip over to the one that's on page five.

Very quickly, what you're looking at here, the very light blue area is the overall coverage of the entire healthcare industry, the green is the coverage of Aetna that was positive and then the red is the

coverage of Aetna that was negative. And the point is that in April, you'll see the spike downward at the time of the incident, but even more importantly, in July when other companies were reporting that they had had a somewhat similar incident, Aetna was mentioned all over again. This thing has legs, and it will continue to dog us for a period to come. Every time a new incident is reported we're also included [with a statement of] "back in April Aetna had a similar incident." So again, kind of a word of warning, there's nothing you can do to make yourself completely protected and invulnerable to an incident, but you really need to be prepared because once one does occur, I can tell you from personal experience that it can be pretty difficult to manage. That's it. Thanks.

TOM: Thanks so much, Fred. So often, we try to make sure that our communications and messages get into circulation so they're passed along without the company's own efforts. Often times, when you face things like this, it happens the other way as well.

Let's go to Toni now, who will enlighten us about GMAC. Toni, it's all yours.

TONI: Thank you, Tom. I have to say -- and I also am appreciating the other two panelists' presentations -- this has been a learning for me in these last 40 minutes or so.

For those of you who don't know, GMAC financial services does provide financial services and products to a number of customers. We provide financing for automobiles; we finance to purchase or lease; we provide insurance products. And we have a mortgage business that provides residential mortgages. So we are in a position of collecting and assessing credit risks on a daily basis. And we collect a lot of information about our customers given the nature of our business.

So, this is clearly an area of the highest level of concern and seriousness at GMAC -- to protect personal information. By the way, let me just also add a little bit of context. GMAC is a wholly owned subsidiary of General Motors at the

moment, although General Motors is in the process of selling a majority of equity interest in GMAC to a group of investors, so shortly GMAC will be more of an independent company. But our association with General Motors is a good one, and we work together on protecting personal information.

We have a personal information security incident process that I would describe as being robust and even award winning, to investigate any incidents and react quickly and decisively to any potential incident involving personal information. It is, as some of the other panelists have mentioned, a cross functional group of people who come together to kind of assess what happened and investigate it and participate in the response to whatever the incident happens to be. Communications is very much a part of that, as are the security, legal, and privacy experts. My chart doesn't show it, but the IT teams at both GM and GMAC have Chief Privacy Officers, and I think we come together fairly quickly and react quickly.

*"... there's nothing you can do to make yourself completely protected and invulnerable to an incident, but you really need to be prepared because once one does occur, I can tell you from personal experience that it can be pretty difficult to manage."*

- Fred Laberge

Also quite often the enforcement of the policies becomes a subject of discussion for those of us on this response team. At GMAC we do have robust policies on data storage and computer encryption. So for example, and this applies to all GMAC employees worldwide, personal customer information is prohibited on any type of mobile computing equipment – a laptop, a storage disc, a blackberry or other PDA. Secondly, all laptop computers are encrypted so this is a policy that we also have communicated broadly to our employees from the top of the company in very clear communications directly to employees.

While we have been fortunate in not having as high profile incidents as some of our peers here on the call, I never take that for granted. And as Fred said, it could happen at anytime, anywhere, to anybody. And so you have to be constantly on guard. When we have had the threat of customer information being lost or stolen, we really follow the Golden Rule and we, of course, notify customers as required and sometimes even as not required. We do it on a voluntary basis. The direct communication with the customer I think is a key advantage.

Most of the incidents – it seems generically or universally, while we may mobilize and react to them and maybe even take action in response to the incident – do not result in fraud or identity theft. So we've heard some incidents of the theft or loss of a laptop wherein the laptop was actually the target of the theft, not the data. So even still, as a company we need to react as if it would be the result of identity theft, even though more often than not, it does not.

So communications plays a role in many of these aspects, but predominantly in the messaging, and in the dissemination of that messaging, and as well as in the internal communication of the policies to our employees. I would like to make a side note on the media relations aspect of this. Frankly, the direct communication to the customer means that we need to rely less on the news media to communicate with them, which I think is a plus in these kinds of situations. We're certainly prepared to respond to news media in the event that there is coverage of one of our incidents, but we don't proactively use the news media as a means of communicating to our customers. We prefer to do that directly. Tom, I can go on, and maybe more of this will come out in the Q&A, but I don't want to use up much more time. I want to make sure we have ample time for questions, so I think I'll stop there and turn it back over to you.

TOM: Okay, very good. Thank you very much Toni, and Fred and also Harriet. Let's go to the Q&A right now, so we do have a good amount of time here to take your questions.

Again, the way the process works now is that for you to ask a question just press zero and then one. An operator will come on the line, take your name and affiliation and then put you on the line to ask a question. So let's go to the line and see if we have any questions.

OPERATOR: At this time there appears to be no questions.

TOM: Okay. Let me maybe kick off and throw one in here, and I'm going to back to Harriet on something that you started your presentation with. And that is the question of providing trust, and what is so essential for corporations to be able to do for their clients who entrust them with their own personal information. Are there any particularly outstanding examples of companies who do a good job in proving that kind of trust? And maybe one or two pointers you can give us all in terms of some specific things that they do?

*"... communications plays a role in... the messaging, and in the dissemination of that messaging, and as well as in the internal communication of the policies to our employees."*

- Toni Simonetti

HARRIET: In the studies I've seen -- certainly in a lot of the reputation surveys -- what it all boils down to is that most people don't roll out of bed in the morning thinking about privacy, or security for that matter. When you deal with a company as a consumer or as an employee, it boils down to, "Am I being treated fairly and am I getting what I want, when I want, when I want it? Am I getting value for what I'm spending or investing in the organization with which I'm doing business or having a relationship?" If you meet that, privacy and security are basically elements of that. And if you surprise a consumer, and that surprise can include, "Oops, we have to tell you that we have potentially put you at risk", that is going to take away from trust, and therefore, create the kind of

consequences that we have been hearing about and reading about, frankly, in the media. All of the consumer research that I've seen really points out that basic insight, which is not exactly rocket science.

And the other is when you get into secondary discussions of what consumers want. There's a pretty well-known segmentation of the U.S. population -- that has shifted a bit over the last couple of decades, but not that much -- it really breaks it down into three segments. One segment is the privacy super concerned, the privacy absolutists, those folks who will never ever give their phone number for subsequent marketing, who will resist those kinds of engagements with companies. And they're roughly between 5% to 15% of the population at any moment, I believe. Another segment would be the ones who are the privacy unconcerned, and those are the folks -- you probably know a few, maybe you are one yourself -- who say, "You want my phone number, sure ... you want this, sure. I'll trade you my DNA for a Big Mac." A free coupon for a Big Mac is another example just used kind of jokingly. But these are folks who don't really care, and the privacy unconcerned at this point has been shrinking over the last decade or so, I think, as a consequence of the environment, and it's probably down now to about 5% to 8% to 10% at any moment. And then the rest of us, the majority of us are more privacy pragmatists. So we're willing to engage in behaviors that uncover elements about ourselves. Sure, I'll trade a little bit of privacy about my shopping habits for value in a consumer-shopping card if I feel that there's value. But the moment that I feel that it's getting to be uncomfortable and not a good balance between myself and the organization, then I'm going to not use it. I'm going to rip it up. And that's the kind of behavior I think that the data breach incidents are creating -- a lack of trust and lack of comfort and uncovering the security risks inherent in what we all do. And that's what I think is causing some of this latest itch or concern.

And I think just looking around you -- companies that are good brands that you think are trustworthy brands, are the ones who are doing it right.

And that doesn't mean that we're not all going to have incidents. It's a matter of how we prepare for them and how we respond to them. As I think the other two speakers articulated, communications plays a key role here, particularly in elevating the folks who are typically concerned with compliance with security standards or legal requirements, that they may not have the full view of how to deal with the corporate reputation and all the various stakeholders that communications typically knows how to deal with. And so that's where the partnership really is key to make sure that the response to the incident is indeed an "A class response," a world class response as opposed to maybe being a few beats behind.

*"When you deal with a company as a consumer or as an employee, it boils down to, "Am I being treated fairly and am I getting what I want, when I want, when I want it? Am I getting value for what I'm spending or investing in the organization with which I'm doing business or having a relationship?" If you meet that, privacy and security are basically elements of that."*

- Harriet Pearson

TOM: I think that's an interesting point too, because that's once again the role of communications corporate counsel process in this.

HARRIET: Exactly, exactly.

TOM: Operator, any other questions?

OPERATOR: We have a question from Mr. Ward White from Marcus Corporation. You may go ahead with your question.

WARD: Hello speakers and thank you very much. This has been superb. My question is really directed to Toni and Fred. Toni, if I understood you correctly, you have the advantage of being able to communicate directly to your customer

or client and therefore do not make a public announcement of incidents, at least sometimes, and I'm not in disagreement with that. Fred, yours was very public and you also had an IR timing question, and you did make it a public announcement. My question is what are the criteria for going public or not public? Clearly, every incident doesn't warrant a public announcement. Do you have any criteria for that? Or I'd be interested in how you think about that question.

FRED: This is Fred, I'll start, if that's all right, Toni.

TONI: Sure, Fred, go ahead.

FRED: In our example, it was really up to the customer. And the customer in this instance was the Department of Defense. Typically, we work with the customer and explain what happened. The most important thing is to be very forthcoming and to explain exactly what you know, everything that you know. Anytime you get new information and it changes, you have that dialogue. We ended up having a dialogue for more than a week and we found that they went sort of back and forth themselves. This is new and difficult for everyone to deal with. Again, not to change the tenor of your question, but it really ended up being the customer's decision that they wanted us to issue a statement. In addition, we obviously did communicate individually with the affected members, and with other constituencies that we thought it would be important to deal with directly. So we didn't use the media to disseminate the message, but we issued a statement as part of the overall communications after having determined that that was the most forthcoming and the best thing to do. But what I'd like to leave you with -- the sort of take-away here -- is that we had thought about this more than a year in advance. We had encrypted the majority of our laptop computers that employees use -- we have about 10,000 in the company, I think -- and we had done a majority of them at the time this incident happened. This one did not get encrypted, it was password protected. We had a lot of other things in place. Employees had been given information

about the importance of this. Despite all of those things, it quickly became a very public issue and again, we also had to deal with facts getting exaggerated and there was never any proof that the information on the computer was misused in any way. It was probably fenced at a local pawn shop. Nonetheless, it got out of hand very quickly. So, be prepared, I guess, is the short version of the speech.

HARRIET: The other aspect here is that you may not be able to decide the timing or whether or not to publicly disclose because the legal requirements in place in most of the United States at this point will probably drive your decision to need to notify. And when you notify more than a few people, it's clearly going to become widely understood.

TONI: Yeah, I think that's a good point. I was going to add that I think the size and scope of the breach plays into a decision as to how public, how broadly you go in your communications. And to the extent that you can communicate directly to those affected by the breach without creating a media story out of it, I think that, for us at least, that's the desired path. To the extent that it's the size and scale of some of these other ones, I think that in some cases you've got to have a fairly strong and probably even proactive communication that goes beyond the affected population.

FRED: Yeah, that clearly would have been our preference but it was out of our control. We needed to do what the customer wanted.

TOM: Okay. Any more questions on the line, Operator?

OPERATOR: At this time there are no other questions.

TOM: Okay. We have just a couple of minutes. Let me throw one in here because I think this is also an equally critical subject to the external one that Ward just asked. This is on the internal, or the employee communication side and I throw this open to all three of you: How do you strike

the balance? And is there a way any of you have found of hitting the right balance after you have a breach -- when you may want to revise and review your policies and put more controls and more security in place -- of hitting the right tone with your employees between having them, in a sense, wanting these additional elements to come into play, versus having it seen as anything from overly concerned to perhaps even somewhat punitive. So how do you hit that right balance on the employee side -- have them understand these things?

TONI: I can start off here, Tom. I think in a company such as ours, we're a financial services company, so I think there's a fairly good understanding that we are collectors of important personal information and we have to do everything in our power to protect that information and use it only in the way intended. And so I think that is just inherent in the way we behave as a financial services company. Personally, I have not seen any pushback from the employee audience to some of the types of security or precautions we've taken to prevent misappropriation of this information. We can all say that it's a little inconvenient. For example, I went through this myself. I had a hard drive that crashed, and we needed to try to retrieve data off of it to put on my new computer. This was my own, sort of day-to-day work data. It was, because of the encryption, very difficult and time consuming to go through that process. Was that an inconvenience? Yes. But did I mind? Absolutely not.

FRED: From our perspective, it was really a matter of sort of kicking it up a notch in terms of the employee awareness. We already had programs in place, compliance and privacy managers would talk with employees from time to time. Everyone has to do an information security online one-year refresher course, or every year one-hour refresher course and those kinds of things. But we ended up getting our CEO on a video that was simulcast to all employees and we did a lot of Q&A and a lot of follow up to make sure that employees understood just how serious it was. Even though, again I emphasize, nothing ever came of it. The

laptop was stolen, but no information ever has been shown to have been misused. Nonetheless, it really can hurt your reputation, so that was what we were reinforcing, that employees need to take this seriously, it's not something they can take for granted. It's not something that was being ignored. It was something that was taken for granted, that the company had adequate protections in place. So I could just go, leave my desk and go down to the cafeteria and not lock my laptop or whatever. And that's changed significantly and it really came from the top down.

*"...the size and scope of the breach plays into a decision as to how public, how broadly you go in your communications. And to the extent that you can communicate directly to those affected by the breach without creating a media story out of it, I think that, for us at least, that's the desired path."*

- Toni Simonetti

HARRIET: I would agree with the other two speakers, but the other dynamic I think you ought to be aware of is all of us as employees will kind of say, "Well what's in it for me and how does it relate to myself?" So it's useful for the company to also be able to demonstrate what you're doing to safeguard the security or privacy of the employee him or herself. So to the degree you can also raise the profile of that, as in, "What am I doing to protect your health information or your insurance information or whatever? Your data that I have, as an employer, is actually good, so there's not dissonance between the corporate requirements for you as an employee acting for clients and customers, versus how the corporation is treating you."

TOM: That's a great metaphor and we'll close on that one. Let me thank everybody for your participation. First of all, Harriet, Fred, and Toni, thank you very much. It was really well done today and you delivered a lot of information to all of us. All of you who called in and participated, thank you very much. I'd also like to thank Paul Basista and Susan Chin from the Arthur W. Page Society once again for their usual excellent work in putting this all together and getting us all together this afternoon. And thanks also to Roger Bolton and Rich Jernstedt and Larry Parnell, who are part of our program team. We do a lot of discussion coming up with the subjects and there's a lot of back and forth, and that's very helpful in putting these together. So thank you, guys.

We solicit your comments on future subjects, as always. If you have any, please send those to Paul Basista. Paul's email is simply [exec@awpagesociety.com](mailto:exec@awpagesociety.com). We're going to do two more teleconferences this year and we want to make sure they're relevant and timely and serve you with some good value in these subjects. So please let us know.

The transcription from today will be available on the Arthur Page website in a short amount of time, so you can pull these down and pass them along to some of your colleagues if you want.

That's it for today, thank you all very much for attending and participating, and we look forward to seeing you for the next one. Thanks a lot and bye bye.

## ARE WE OUR VENDOR'S KEEPER? NOVEMBER 1, 2006

### PAGE ONE PANELISTS:

**Dr. Michael Josephson**

Joseph and Edna Josephson Institute of Ethics

**John Budd**

The Omega Group

**Kirk Stewart**

APCO Worldwide

**Moderator:****Tom Kowaleski**

TOM: Good afternoon everyone, or good morning to you as well. My name is Tom Kowaleski, and as a member of the Board of Trustees of the Arthur W. Page Society, and on behalf of the entire Board and our President, Roger Bolton, I'd like to welcome you to our third Page One Teleconference of the year. In keeping with our intent to have a series of discussions on current subjects and trends and issues that can affect all communications leaders and are therefore important to us all, we've titled today's subject "Am I My Vendor's Keeper?" The recent significant play around the investigation of HP's use of outside suppliers has made this a particularly timely subject, but our discussion today is not intended to focus on HP alone. Rather, when this case came to light it also illuminated the fact that daily corporations are faced with the realization that when they entrust suppliers with work, they are also entrusting them with their image and reputation. And in a world where we live today with downsizing and outsourcing and even delegating large chunks of what had used to be considered a core competence, it's becoming ever more common to ensure that your company has comprehensive and clear guidelines of ethics and integrity in place for your suppliers. But really, is that enough? And while speaking of that, what's the role for all of us as communicators? How should we be involved in

this process -- since when it does go wrong -- we are thrust into the center of the issue?

And as we all know, this is not a recent phenomenon even though it is now a hot media subject. In the coming hour we're going to ask you to join us in a discussion with three experts who know this subject very well, and who have all been on the line in various ways of this issue when it has hit them and consequently have an excellent perspective and sound advice for us all.

Our first guest today is Dr. Michael Josephson. Michael is the Founder and President of the Joseph and Edna Josephson Institute of Ethics. He's one of the nation's foremost ethics consultants to major corporations, governments, media organizations and law firms, and over the years Michael has led more than a thousand ethics programs. Many Page Society member companies have worked with the Josephson Institute. Michael was a regular and recognized ethics expert by many of the nation's leading print, radio, and TV outlets, and has been a law professor and educator on this subject. He's also a published author of several books and articles and he's won a number of prestigious awards for his work and contributions in the field. So I'm sure he will have a lot of excellent insight for us today on the ethics question.

Our second panelist is Kirk Stewart. Many of you know and are friends with Kirk and we're delighted to have him as a participant with us today. Kirk is Executive Vice President and leads the corporate communications practice at APCO Worldwide. He spent eight years at Nike as the Global Vice President of Corporate Communications, and there he was responsible for corporate relations, brand communications, crisis and issues management, internal communications, community affairs, sustainable development, and stakeholder engagement. He also led Nike's Global Responsibility team. Prior to being

at Nike, Kirk enjoyed a successful career in the public relations agency business and was Chairman and CEO of Manning Salvage and Lee. While at Nike, Kirk was on the leading edge of a major issue dealing with the company supply base, so he brings a great deal of experience and insight to our discussion today.

And our third panelist is John Budd. And John brings to us over 50 years of varied and significant communications knowledge and experience. He's a veteran of both the agency and the corporate world, having been Vice Chairman of Carl Byoir and Associates, and working and counseling thirteen Chairmen and CEOs during his tenure in both the corporate and the agency business. John has written nine books on excellence in communications, governance, media relations and personal growth, and was a long time columnist of *Plain Talk*, taking on subjects ranging from credibility to corporate initiatives. Particularly germane to today's subject however, John is a member of the National Board of Advisors of the National Association of Corporate Directors. And he's a Director of the New York Chapter of NACD as well. Therefore, John's perspective of Board activity on the subject will be enlightening I'm sure.

So we're going to start our conference today with a bit of discussion with our three panelists and then open up the phone lines for your questions. And when we do this I'll explain the procedure for calling in and identifying yourself. Those of you who have been with us before know that it's pretty simple to do, and it's quite a good thing to be able to get a chance to talk to our three panelists here today. What I'd like to do is to get started by jumping off on the subject that prompted this conversation. The kinds of things that I would be really interested for all of you to open the discussion with is the current news about HP. Do you think that this will have an effect -- or is it already having an effect -- on corporations, maybe going back and reviewing how, what, and with what direction they hand off work to suppliers?

So why don't we kick off with that one and I'll ask our three panelists if they'd like to get the ball rolling on this one.

JOHN: Well, I'll open up with a question: Who is the "I" referred to in "Am I My Vendors Keeper?"? If the "I" refers to the corporate executives, the CEO, or the directors, then I would suggest that public relations does not make policy but rather, it reacts to it, largely. If it refers to PR as being the vendor's keeper, then I think that's presumptuous. So I think we should define who the "I" is.

*"In the court of public opinion, whether or not it's true in the court of law, you in fact will be held accountable for the conduct of your vendors..."*

- Michael Josephson

MICHAEL: This is Michael Josephson, the -- I guess -- designated ethicist. I viewed the "I" as saying is it a corporate responsibility that maybe the communications professional has a piece of. And I think in some ways the question is rhetorical because the obvious answer is you will be held to be your vendor's keeper in the sense that if you have a vendor, or for that matter any close affiliate, who does something highly ethically questionable or illegal, there's no question that your company or organization will be in the news. And that means the communication professional is going to have a responsibility with regard to how that is handled. I think the earlier that the communications professional can be in on some of these considerations, and the more comprehensive a company has standards so that they don't get into trouble, the better. But I think the answer is very simple. In the court of public opinion, whether or not it's true in the court of law, you in fact will be held accountable for the conduct of your vendors, as in the case of HP.

KIRK: I couldn't agree more with that. And I think what's happened recently with HP has,

hopefully, raised the level of awareness among a lot of companies about the depth and breadth of all the potential areas of exposure they may have, and in some cases may be ones that aren't quite so obvious as the HP situation. If there's a silver lining in what's happened, I think it is that this has created a level of awareness of these kinds of issues all the way to the board room. And I think the other thing is that it's certainly highlighted the impact that an incident like this can have on the reputation of an organization.

JOHN: There are two levels of awareness. One is the awareness of the difficulty, and the other is a sensitivity to or awareness of what should have been done. Now what Michael Josephson said, I agree with theoretically. But its interesting to note that the offices of public relations of Hewlett Packard pointedly and publicly said that the PR departments role was merely, and I'm quoting "to serve as a conduit of information" end of quote. Now that's a damning bit of candor. I wonder how broad that is across industry.

*"...the beautiful thing about a communications specialist, they can see through the eyes of the external stakeholders better than anybody else who gets internally involved in a process."*

- Michael Josephson

MICHAEL: But that may be how the company designated it, and I don't doubt that the role is determined, obviously, by your client. I think the broader question for us is what should the role be. There's no question that the communications professional is going to have a response obligation when these things occur. The real issue is could one handle these things better if we anticipated them better, and shouldn't enlightened companies find ways to bring the communication professionals perspective to the decision making table at a much earlier stage. And I say yes.

KIRK: Yeah, this may be wishful thinking on my part, but I would like to believe that had a communications professional been involved in the decision to investigate board members, to investigate employees, and above all to investigate journalists, I would [like to believe that] the communications professional would have at least raised the issues about how this gets perceived by external stakeholders, and what the ramifications would have been for the company when it became public. Now again, that could be wishful thinking on my part, but I've got to believe that anybody on this phone who would have been told that this was what was going to happen, would have at least raised a couple of questions and a couple of issues about the behavior.

MICHAEL: But it's not just raising the issues, remember, the first guy who lost his job was the ethics officer.

KIRK: Right.

MICHAEL: Because the ethics officer went along with it despite his reservations.

KIRK: Correct.

MICHAEL: We not only need professionals who raise the issues, but sometimes put stakes in the ground and say, "Look, I'm going to tell you there's no way this is going to be acceptable to the public. There is no way." See, the beautiful thing about a communications specialist, they can see through the eyes of the external stakeholders better than anybody else who gets internally involved in a process. And if they're competent at all, they would have said, "This is a disaster," and hopefully they would have said it firmly enough and not with just a shrug of the shoulders and an "okay, I warned you."

JOHN: It's a question of what they see through what eyes. Do we know -- or can we speculate -- that the PR department at Hewlett Packard knew about this investigation, or did they learn of it only when it started to hit the fan?

KIRK: Again, I don't have any insight into this any more than anything else anybody's read, but I'm assuming since one of the people in the PR department was one of the persons investigated, I'm assuming they found out about this afterward.

JOHN: Afterward, I agree.

TOM: I'd like to move into a little more strategic area around this question because I think this is pretty fascinating. But not just with regard to HP though. Many companies today do have a tendency to believe that if they have standards and practices around ethics and integrity that are well written, and those standards and practices are then communicated either contractually or verbally when they entrust suppliers to do work on their behalf, that that's -- in a sense -- 90% of the job, and therefore [the companies believe] that the supplier is forewarned and cautioned and made informed of what's going on. It seems to me that there is some role here for the communications leadership to play, in a sense of some follow up of this, or oversight. Now, in a large corporation that's darn difficult because suppliers are in such high multitudes of work and doing so many different things. But do any of you see that as a plausible opportunity where communications should be involved and kind of managing this as an oversight standpoint?

*"I can tell you that sitting - as I have been for the last dozen years - with directors and senior officers and so forth, the term "public relations" is rarely ever mentioned."*

- John Budd

JOHN: In every company, no matter how enlightened, generally the CEO has a hierarchal structure. And the PR department is not sufficiently positioned on the food chain so that they can take the initiative to raise issues like this. It won't happen. I can tell you that sitting -- as I have been for the last dozen years -- with directors and senior officers and so forth, the

term "public relations" is rarely ever mentioned. Whenever I have anything to contribute I do not put it in the context of public relations because if I do I can see their minds churning to spinning, manipulation, and all the things that we detest. So I have to make my points on the basis of the logic of them, period. And I would suggest that the PR department, Hewlett Packard being a case in point, was probably shielded from what was going on until it happened.

MICHAEL: I guess the first thing is the premise about standards of conduct, as someone in our organization is often asked to write or review those. They are almost always consistently ineffectual. Standards of conduct are there to protect you legally; they almost never control behavior unless they're quite specific and enforced. The fact is that HP had good standards of conduct, and, in fact, they have a good reputation for their conduct. But all of a sudden the Chairman wanted to get something done and everybody turned a blind eye, and willful blindness occurred. What you need is an ethical culture, and you need consciences in an organization. Now, that shouldn't be the exclusive province of the communications professional; legal counsel should have that, so should HR, so should everybody. But someone within that organization -- if not everyone within that organization --, has to ask themselves, "Are we in keeping with the spirit of standards of conduct?" Not with the letter of the law, and not some legalistic rules-based notion, but a values-based notion of whether we are living up to the reputation and earning the trust that our public wants and expects of us.

KIRK: I completely agree with Michael here. I think this goes way beyond standards of conduct, and I'm sure we're going to get into the pluses and minuses of standards a little bit later. But I really do believe this is about a company's values and their value statements and their value beliefs. If communications can play any role in this process, I think it is to make sure that the organization fully understands what those beliefs are, what those operating principals are, and what those values are, that the company shares a way it's

going to operate. Again, I think if there's a role [for communications] here, that it takes place before any kind of behavior ever takes place. I think that it's the role of making sure that the organization's values are clearly understood and communicated inside the organization.

*"If communications can play any role in this process, I think it is to make sure that the organization fully understands what those beliefs are, what those operating principals are, and what those values are... making sure that the organization's values are clearly understood and communicated inside the organization."*

- Kirk Stewart

TOM: And I agree with John that sometimes corporations don't always keep their communications people informed, or don't want that from them. I think part of the focus of this call is whether that is a healthy thing, and if there should be more affirmative advocacy. The reason why it's a very natural function of a communications professional is because the communication professional's whole job is to perceive things from the perspective of a lot of different stakeholders. And therefore, while marketing people are looking at one thing and production people are looking at another, the communications professional intrinsically has at his or her fingertips the concerns about how will this look, and therefore they are a natural person to want their experience at the decision table.

JOHN: That's what you say, but that's not what CEOs necessarily say and certainly is not what Directors think. It's my contention that the PR department at Hewlett Packard lost the ball game when Mark Hurd became CEO. That was the critical moment when they should have written a persuasive memorandum to the CEO analyzing the past mistakes which included leaking and bad press and so on, and recommending how this

could be avoided or at least ameliorated by certain actions. They obviously didn't do that. Hurd, looking at all of the problems of Hewlett Packard, identified those that he thought were important and was rebuilding credibility, profitability and morale. He ignored the public relations function, probably thinking he's got it covered, we've got a person in charge. Instead, he should have been focusing on that and asked, "What can we do differently and better?" which involved him being involved. And he didn't do that. They didn't take the initiative. All of what Michael and Kirk have said is true with the one exception, which I have always said hampers public relations: it is not enough to know what to do, it is not enough to know how to do it, it is not enough to know when to do it, it is the critical issue of persuading people who don't want to do it, to do it.

TOM: You know, if you come back to where so many of these discussions take place inside of corporations – and I think we all agree that this is right at the top of the C-suite – if you were to look around the room, it would be natural that you would probably have the legal staff there, often times the financial staff, in addition to the chairman, the CEO, the president and the senior-most leaders of the company. But, any of us would agree, it's not normal to have the communications person there. And I think the question I would ask all of you is, "What do you think is the reason for that and what are the kinds of things that communications leadership has to do differently to be included in those conversations?" Because often times it's tough to push yourself in.

JOHN: This is a perennial problem. One of the answers, of course, is to think like a businessman, immerse yourself in their world, in their mindset, and be a contributor. Too often the public relations/communications department focuses on the sibling of public relations, which is communications. They do not see the role as we see it.

TOM: Well, often times the role is characterized as a staff function rather than one that is much more involved in the whole strategic direction, the conscious and the being of the company.

KIRK: But that may be one of the markers of companies who are much more sensitive to that. I know of a number of communications professionals. For instance, I've had a lot of work with Johnson & Johnson, where Bill Nielson – just recently retired – was, for a great deal of the time, very much at the decision table. And I think Johnson & Johnson has maintained a fairly good reputation because they're constantly getting that perspective. You can't force a CEO to do it, but I think self interest is driving them in that direction now because someone needs to be bringing that perspective. If not, pay me now or pay me later.

JOHN: Let's not forget that Jim Burke was an extraordinary executive. The Business Roundtable, representing 100 to 150 of the top CEO's of the top companies, in a paper that laid out the guidelines for shareholder communications, which is certainly in the province of PR, said, and I quote, "The board should specifically designate a member of management such as the Corporate Secretary, the Head of Investor Relations, or the General Council to"... so on and so on, "to do the communications to shareholders." Nowhere is there a mention of public relations. These are the guidelines to all the CEOs. It's no wonder that they don't think of Public Relations in the context that we do.

MICHAEL: Well, I think you've just outlined it, John, with that statement. And it comes down to this: some companies are very enlightened when it comes to that, and some are probably less so.

KIRK: Just one other comment. I would say that the companies that choose not to have communications at the table will eventually pay the price for that.

MICHAEL: I agree.

JOHN: Will they know it?

MICHAEL: Only afterward.

KIRK: Trust me, they'll know it afterward.

MICHAEL: But people learn. I mean this kind of event. I think HP has been sort of the Watergate event at a very high level because it's not at all an incidental fact that this was a Chairman of the Board – which is an unusual kind of situation – who really was controlling all of these things.

KIRK: Yeah, agree.

*"... often times the role [of communications] is characterized as a staff function rather than one that is much more involved in the whole strategic direction, the conscious and the being of the company"*

- Tom Kowaleski

TOM: Let me switch gears here just a little bit and take a look at this issue from the outside-in a bit. And that is, today when we look at suppliers, it's often simple to think that you communicate to a supplier who is doing work on your behalf, but we've often seen instances where there are several tiers of suppliers doing work on your behalf. And even if you do an adequate job of communicating to them know your ethics, your integrity, and what you expect of them, you're often times only communicating that to the first tier. And there are then several others in the supply chain who also will be in the position to be speaking for you. How does a company really effectively manage that in terms of making sure of that communication? We touched a bit on the communication inside the company setting the standards. But how does the company make sure it goes down that supply chain? And what's the role of communications in making that happen?

MICHAEL: Well, before you get to what the communications person is, it's first the corporate responsibility – whether it's legal counsel or auditors. And I think the first thing you've got to do is prioritize risk. There are some relationships that have inherently far more risks in them than others. A sub-sub-contractor generally presents you

much less risk than a major, major contractor who's a deliverer of one of your key products. So I think you have to assess risk and the higher the risk, the higher the vigilance. You may have to have audits, you don't just have them sign an agreement and assume that they'll do that. If they're going to do wrong and illegal things, they'll sign an agreement. The point is is that you may have to audit it. But the real test is this: What will the public hold you responsible for? If it's really very, very remote -- the public's not totally irrational -- they'll understand that it's remote, that this is a person who sold the cardboard boxes and they violated labor laws and probably nobody will hold the company responsible. But if they're the ones who are making one of your key products, you have to ask yourself realistically: If someone messes up, will it come back to my door? And if it does, you better think about it, you better talk to the people, you better know the people, and you better audit the people because they are your people.

TOM: Kirk, this falls into an area where you've had some past experience I would assume.

MICHAEL: Yes.

KIRK: I would echo Michael's comments. I think that you are responsible for the things that external stakeholders can reasonably hold you responsible for, or believe you're responsible for. And I think that's the primary test.

MICHAEL: And then you have to set up whatever structures you need to, and that's where you need other people. It's not by any means purely the communications professionals' responsibility.

KIRK: Not at all, not at all.

MICHAEL: But it's the communication professionals' responsibility to ask, "Have we done this yet? Have we done that yet?"

KIRK: Right.

TOM: Kirk, when you were at Nike, you had a situation -- if not a couple of situations -- that fell very much into this area. Talk a little bit about some of the things that you learned from that, and tell us about some of the practices that you put into place that might be helpful.

KIRK: Oh boy, how long do we have?

TOM: Well let's narrow that down a little bit here. How about ...

JOHN: Why don't you just tell us the impediments to the golden rules that you had in place?

TOM: How about in the area of transparency? I think you probably did a lot in that area after some of the situations that you faced. Are there some good guidelines here that we all should be aware of?

*"I think that you are responsible for the things that external stakeholders can reasonably hold you responsible for, or believe you're responsible for. And I think that's the primary test."*

- Kirk Stewart

KIRK: Yeah. I think that from Nike's perspective, and maybe this applies to other organizations as well, I happen to believe that increased transparency equals increased credibility. Again, just reflecting on the Nike experience, when the whole supply chain issue became as big an issue as it did, I think the company had very little credibility to speak on its own about what was going on in the supply chain. And I think that one of the ways that the company began to make some progress on that issue was to be more open and transparent about the process that was in place. Michael sort of touched on some of those elements of that process. But the company got to be much more open and transparent about the process and began to self-report its own violations. And we can talk about self reporting here

in a minute, but self reporting completely takes away the 'gotcha factor' that I think a lot of companies suffer from when they've got some supplier-conduct issues. And so I think that this whole issue of transparency is really important.

*"I happen to believe that increased transparency equals increased credibility... self reporting completely takes away the 'gotcha factor' that I think a lot of companies suffer from when they've got some supplier-conduct issues."*

- Kirk Stewart

JOHN: I don't think we're giving enough attention to the difficulties a public relations person, in general, has in getting the attention, respect, and so forth of the CEO for what we are talking about as being so logical. You have to fight for every little bit. When I was in the corporate world I wrote a story on an 8K announcement which indicated we had found some illegal payments overseas. They were a bunch of curmudgeonly Yankees, and the Chairman was horrified that I would write a negative story, and I said it's going to come out anyway. So he said well, "I'll talk to Jim." Jim was the head of the board's audit committee, and he overruled me. He said, "Oh, we're never going to put out a story like that." So I retreated to my area and I just collected clips as they moved across the country. When it got to California I knew that was the end of it. So I went into the chairman's office, put them on his desk and said, "Now look. What should have been an overnight to one-day story, has been a two-month long feature. And it's a two-month long feature because you tried to finesse it." And I never had trouble with them again. But it's a constant battle -- it is not a given.

TOM: Well I think that this has been a subject that we have spoken about here quite a bit today, John. That is, it starts at the top of companies; it starts with the respect that the function of communications has. Also on the other hand -- to be

very fair -- it's also the advocacy that the communications person brings to the job, and that the staff brings to the job, to continue to, as you say, fight that battle.

JOHN: Daily.

TOM: But I'm not so sure -- unless anybody else thinks differently -- that there is a set of guidelines that every communications department would follow or could follow.

JOHN: No, I think it's very individual.

TOM: Yeah. Kirk I'm going to go back a little bit to this point of self-reporting to take away the "gotcha factor" because that does seem to be a trend, or an action, that more and more companies are adopting and with very good results. Is there something that you see in your work that makes you wonder why even more companies don't do that? Or are there some impediments that you may see to that?

KIRK: Well that's a really fascinating question. I think that initially, most companies probably don't want to believe that the things might be as bad in the supply chain as they might have imagined. And so I think there's a certain amount of self denial that goes on inside the organization. But again, speaking from a Nike perspective, once the organization began to realize through its own internal process and its own internal monitoring that, in fact, there were some issues in the supply chain that needed to be addressed, I think that once there was that realization then the whole issue of self-reporting became much less of an issue. Not only issues in the Nike supply chain, but literally in every other apparel and footwear manufacturer's supply chain and this obviously is not confined just to those two industries. But I think once Nike got comfortable with the fact that in fact there were issues that needed to be dealt with, the issue of self-reporting became much less of an issue. Again, the company was also in a situation where if it didn't self report, others were going to report for it. So you have to decide whether you going to stand back and let

others define your process, define your supply chain, define the issues, or whether you are going to try to define that yourself.

The other thing I would say is that I think that there's a lot of concern, initially, about, "Oh my goodness, we can't possibly be that transparent and here are all the negative consequences that are likely to come about through this level of transparency." And I think at least one of the lessons that I learned is that rarely are the consequences of transparency nearly as dire as management may want to initially believe. And I think whatever negatives they are, at least in the Nike situation, the positives far outweighed the negatives.

MICHAEL: There's another major factor and I think my profession is part of it. I was a law professor for 20 years and a lawyer and I think your legal department almost instinctively reacts negatively to any negative disclosures.

KIRK: Right.

MICHAEL: Because as someone who taught litigation, it doesn't help you in your lawsuit, it never does, to make those admissions. And on the other hand, there's also this hope-against-hope that maybe no one will find out. And so the hope that no one really will find out, and the obvious legal consequences to doing it, has elevated short term considerations above long term because it is obvious that the perceived cover-up is always worse than the crime and open disclosure is always perceived better in the long run. But that doesn't mean you don't pay the price. And, by the way, legally we're moving to that. With Sarbanes-Oxley, the federal sentencing guidelines, there are a whole new raft of things that are mandating self-disclosure, so you won't even get any ethical credit for it anymore.

KIRK: Correct.

TOM: Isn't this a major incongruency that's really going on today? Because what Michael just said is probably the same thing that John, when he began practicing public relations 50 years ago,

was probably hearing senior management say. Yet today, everybody knows that we live in a world where the ability to report, the ability to find, and the ability to spread news information is so much greater than it ever was before but we still kind of hold to old truisms in a world with a new defined reality.

JOHN: Yeah, it's also faster.

TOM: Yeah, exactly. Exactly.

*"... your legal department almost instinctively reacts negatively to any negative disclosures... it doesn't help you in your lawsuit, it never does, to make those admissions."*

- Michael Josephson

MICHAEL: And it's more inevitable. It is just simply inevitable that somebody on a web blog can copy your documents and do everything. The good thing is it takes away the naiveté so the question is not whether it comes out but when, and whether you're positioning it forwardly in the context of what you're going to do about it. Look, no matter what we call the law of big numbers, if you have enough people, someone's going to mess up. You can't always blame a company because somebody messes up. But you look carefully at how the company dealt with it when there was a mess up. And if the company looks accountable, looks responsible, is handling it with diligence, that's all anybody can expect.

KIRK: Yeah, I don't think that any reasonable stakeholder expects perfection. And certainly in the Nike place, when you're dealing with a supply chain of 800 factories and five or six hundred thousand workers, no one expects perfection. But I think there is an expectation that there's a process and protocol in place, that there's some sort of monitoring and sanction program in place, and that the company's dealing aggressively with the issue. And I think that's where you begin to get the benefit of the doubt when issues do arise.

TOM: Michael, you mentioned the phrase “position it forwardly.” What are some of the great ways you’ve seen that being done? And I don’t mean just specific examples, but companies that sort of take these kinds of issues and get out in front of them?

MICHAEL: Well obviously, because it’s classic, the Tylenol situation at Johnson & Johnson. But there are many other situations where companies have to acknowledge that, “Something went wrong, and these are the steps we’re taking to solve them.” And that’s the thing, but when I say “position it forwardly” I mean, “What have we learned from this?” The problem is that most companies spend the first two or three press conferences saying, “We have to study the issue. We don’t really know enough about it yet, we have to study it,” but they know enough already, and it’s just a delaying factor which gives the news media more fodder to pick up on. And so the idea is – were it Watergate – you look at that again to say, “What an incredible mess up. We’ve taken steps to not only reprimand the people or fire those who did it, but we’ve now set the policies so that this won’t happen again.” If I had the workforce problems that Nike had, I would have much more immediately urged that they said, “Look, we didn’t give this as much attention as we should have, and now we are. This is our policy, and this is what we’re doing going forward.” It would end the matter.

*“... everybody knows that we live in a world where the ability to report, the ability to find, and the ability to spread news information is so much greater than it ever was before...”*

- Tom Kowaleski

TOM: Okay. Let’s open up the phone lines now. For those of you who have a question, simply punch zero and then one, and that will put you in the queue and the operator will come on. Please identify yourself and your affiliation and then the operator will introduce you into the conversation and we’ll get right to your question.

While we’re waiting for that, John, I’ve got a question and a little bit of it goes back into the role of boards. From what you’ve seen and observed and have been involved in, when boards make the decisions to take action and to do certain things that may include involving outside suppliers, do you see boards making sure that the communications department is informed of what some of their actions are, to make sure that if things break or news happens, that people are already in the loop?

JOHN: No, they never go that far. The board’s primary responsibility is to ask questions, to ask the right questions often enough so they get the right answers. They’re quite concerned about micromanaging. In the Hewlett Packard case, they were assured at the beginning, if Patricia Dunn is straightforward, that the people engaged in the investigation were under the rule – that they had to do it ethically according to Hewlett Packard’s guidelines. What happened, I guess, is that they didn’t follow up and see that that was done or they ignored signals that indicated it wasn’t being done. But when a Board makes a major decision which they debate back and forth, when they have agreed, they are so worn out from the mental exercise that it’s finished. I have said so many times, and they sort of patronize me, as Churchill said, “It’s not the end, it’s only the end of the beginning.” They have a responsibility to see that the act and the policy action is presented to the public and to those constituents who it affects most, in the best possible manner to thwart misimpressions. But they don’t do that. They assume it will be communicated. And we all know that just saying that it will be communicated leaves a lot of open questions. They never get into it. Their training, their education, their career paths have never put them in that position.

MICHAEL: Well, sadly, that’s often true even for the CEO.

JOHN: Of course.

MICHAEL: I mean this delegation of authority down is, “Look, I’ve got to trust other people will handle the little things.”

JOHN: Right.

MICHAEL: One of the most significant things about Sarbanes-Oxley is the requirement now that a CEO sign-off, at personal risk, at criminal risk, to things that he would never personally know about, but he'd better put heavy pressure on the people below him.

JOHN: But, Michael, that sign-off relates to financial disclosure.

MICHAEL: Right.

JOHN: It does not cover the issues we're talking about.

*"One of the most significant things about Sarbanes-Oxley is the requirement now that a CEO sign-off, at personal risk, at criminal risk, to things that he would never personally know about..."*

- Michael Josephson

MICHAEL: I only meant it sort of as a model of the notion of holding people accountable for things that they just say, "Well how do I know?" Well, you'd better find out, or have total confidence in the people who are telling you.

JOHN: They don't carry it that far, and as a matter of fact, that certification, swearing on a Bible that "I'm telling the truth" is really an insult to honest CEOs, who when they took the job, assumed that responsibility without question.

TOM: Michael, here I would interject the term "plausible deniability" into the conversation because it seems to fit with just what you were saying with regard to Sarbanes-Oxley, and John, with what you were saying as to the specificity of that. What about plausible deniability? Does it have any role still today in corporations?

MICHAEL: It's a phony construct. It came about at the same time we learned about disinforma-

tion, which is a lie. I mean, plausible deniability has this one simple potential legal aspect: In some crimes, I have to prove actual knowledge. And if you've set up a structure that makes it hard for me to prove actual knowledge, it may turn out to be a legal defense. But now there's even a response to that called "willful blindness". If you didn't know because you didn't want to know we'll treat it as if you did know. The ethics of this is simple; the legalities are a little complex. You should know what you need to know or have people who you can totally trust.

TOM: Okay, then we come back up to the chain and the ability to know what you need to know and the role of the communications person in that area. That goes back to what we've been talking about a lot here today, which is: How does communications better get themselves into this process?

KIRK: Tom, I don't know if you've got a question in the queue here, but I have a question for John and Michael. Has your experience been that companies who have corporate responsibility committees of the board or ethics committees of the board, behave any differently than companies that don't?

MICHAEL: That's not my experience, but I've never seen an effective one set up. Everybody just assumes that we're ethical. Like the *New York Times* thought nothing could ever happen to them until it had Jason Blair. And every company says it can't happen here until it does. The truth is that real, real ethics protection is in its infancy. Most ethics officers aren't very effective; most ethics codes aren't very effective. The organizations that are effective develop an ethical culture, and that's a much more complicated thing.

KIRK: Right, I agree.

JOHN: I'm thinking Enron was celebrated for its ethics.

MICHAEL: At least by itself, yeah.

JOHN: Well, Fortune made it one of the most admired.

KIRK: Admired companies, yeah that's true.

JOHN: And later, when [Fortune] called it one of the best companies to work for. You've got a board -- or you had a board at Enron -- which was right out of central casting. I mean prestigious, knowledgeable, every criteria that you would want. But they were also very passive.

KIRK: Yeah, just a slightly different perspective on that, from my experience at Nike. Nike set up a corporate responsibility Board in 2001 as a committee of the board. I've got to say, though, that did in fact elevate the discussion of many of the things that we've been talking about today to a much higher level than they had been discussed previously.

MICHAEL: I wouldn't be surprised, because they were responding to a real experience.

KIRK: Right.

MICHAEL: And the relevance of it was so evident that the people took it seriously. But try to form that same board in a company who hasn't been in trouble yet.

KIRK: No, I think that's fair.

MICHAEL: Look at audit committees. You know, until you have audit crises, the audit committees are passive.

JOHN: Right, absolutely.

TOM: Well, Michael, on the point of companies having ethics departments -- or corporate ethicists -- and the role of the person in that position, did you in any way suggest that often times you think those are started because there is some lack of ethics deeply ingrained in the culture of the company?

MICHAEL: No. I think most of the time they're started because of a compliance concern. And

there's an industry who's very concerned with compliance and they put somebody in. Just yesterday, I finished a two-day program with the Department of Defense and the whole focus whether we can shift what we call a rules-based ethics initiative to a principles or values-based ethics initiative. And that's a whole culture shift for them because when it is rules-based, most of the ethics officers are concerned with not violating laws and rules. They're compliance officers, but they just added the word ethics. Ethics is about values and that's a much more complex thing, and as a result, often fairly low-level people who don't necessarily have the trust are appointed. They are in the ear of the CEO and all they're trying to do is to be sure that everybody crosses the "T" and dots the "I" and it not only doesn't make ethics, it encourages gamesmanship on the theory that if it's legal, it's ethical.

*"... now there's even a response to [the term "plausible deniability"] called "willful blindness". If you didn't know because you didn't want to know, we'll treat it as if you did know... You should know what you need to know or have people who you can totally trust."*

- Michael Josephson

TOM: Yep.

KIRK: Agree.

TOM: We have a couple of questions in the queue, so let's go to the first one.

OPERATOR: The first question comes from Mr. Larry Parnell of Hill and Knowlton. Please go ahead sir.

LARRY: Good afternoon everyone, I've enjoyed this session very much. Earlier you touched on a couple things that I thought were important. One was this whole concept of a seat at the table and

impact and who is in the room and who isn't. And finance and accounting was and PR wasn't. In that context, I'd like to get the thoughts of the panel on what the views are that, during this entire crises at Hewlett Packard, the stock performed extremely well -- in fact, outperformed the industry. I'm wondering if that is good or bad for making the argument that reputation effects valuation.

*"The shareholder wants two things. He wants an appreciation of his investment and he wants dividends... [Shareholders'] primary interest is not on ethics, its not on transparency, it's on what are they getting. And if they're satisfied with what they're getting, they're going to tune out the other things."*

- John Budd

JOHN: Yeah, I'm so glad you said that because I've long believed what we argue about and debate is almost an in-house concern. The shareholder wants two things. He wants an appreciation of his investment and he wants dividends. There's no one size fits all with shareholders. Some are short term; some are long term. John Bogle, who is the legendary founder of Vanguard Mutual Funds, says that shareholders are renting the stocks. They don't stay around very long. Their primary interest is not on ethics, its not on transparency, it's on what are they getting. And if they're satisfied with what they're getting, they're going to tune out the other things.

MICHAEL: But there are more stakeholders than the shareholder and that's the problem. Not every single scandal is going to affect valuation but some of it will affect morale, and morale will affect recruiting, and it will affect the quality of the people you get and keep. We've had resume fraud problems, for instance, in some large corporations which didn't affect the stock but really shook the corporation in a major way. Trust is a very important concept and you can't always expect it to play its role in the stock market,

but I'll tell you it's never a good thing for a company to be involved in news media where they look like they're scurrilous people.

KIRK: The other distinction I would make is that while the HP situation is certainly fascinating to sit and watch and read about, the reality is that what happened there is not fundamental to their business.

TOM: Exactly.

KIRK: And it has nothing to do with how printers or made or how computers are made. It's obviously an issue of values and ethics. But fundamentally what occurred is not central to their business and I guess I would argue that -- going back to Michael's comment about assessing risk -- I think the bigger risks are around those areas that people perceive as being fundamental to the operation of the business.

MICHAEL: But here's another risk: HP is now in the sights of the media in a way it was never before.

KIRK: Oh, I agree with that.

MICHAEL: And they're going to look and find, in all likelihood, some ethics or other issues that they might have not looked for before. So it's a secondary vulnerability.

KIRK: Well they definitely have stepped into the spotlight and we all know how bright that can be.

JOHN: Michael, to your earlier point, I am running a luncheon program in December for directors, the title of which is "Setting the Tone at the Top." It is our contention that directors have a direct responsibility to do that. Now, in a meeting in Washington where there were a whole bunch of directors sitting around a table, it was unanimous that that's their responsibility. What wasn't unanimous, as was clear by the great silence [in the room], was, "What is the tone? What do you mean by that, how do you do it?" They haven't got a clue.

TOM: Larry, thanks very much.

LARRY: Sure. I just want you to understand the context of the question is not doubting that this is an important topic, but that that makes it that much more difficult because you're trying to get the attention of the people that make the decisions about how to conduct the business of the company.

MICHAEL: Although, I'd bet within the company, this was an earthquake.

JOHN: If it was such an earthquake, why hasn't Hurd addressed the issue?

MICHAEL: Well he's testified, we won't get into all that, but the point is it's been an issue for the company and the point was made earlier -- I think well said -- that this is the problem with this kind of a situation. It puts you in the spotlight and now you've got people looking under every rock and behind every tree for the next issue.

MICHAEL: The downside, if not this thing by itself, but what does this say about the company? And what does it create among competitors and other people with the opportunity to leverage that? So that's the issue.

KIRK: This may not be the end of this story. This may be the beginning.

MICHAEL: Exactly.

JOHN: That's what I said before.

TOM: We've got another caller on the line, let's take that call now too.

OPERATOR: The next question comes from Mr. Tom Martin of ITT, please go ahead sir.

TOM MARTIN: First of all, I think it's been a very lively discussion and thanks to all of you for your insights. My question, you haven't really talked a lot about the perception of PR and its own ethical house, and I think going back to some of what John was saying about the percep-

tion of public relations by boards and CEOs, I would just like to hear what the panel thinks about how PR itself is perceived in terms of its own ethical behavior and how that affects its credibility in the C-Suite and at the board table.

MICHAEL: You know, as a non-PR guy -- the outsider -- I think in a lot of the public eyes, you're just one step below the lawyers.

*"Not every single scandal is going to affect valuation but some of it will affect morale, and morale will affect recruiting, and it will affect the quality of the people you get and keep."*

- Michael Josephson

JOHN: Yeah, you want to talk about Fleishman Hillard and Ketchum.

MICHAEL: Well, I mean, the normal notion or idea of a PR person is a flack. You know? And I know at the highest professional level, that's not true. But that is part of the perception and that's why I never use "public relations." I keep calling you "communication professionals" because I think you'd be better to sort of separate from the phrase. But I think the fact of the matter -- the assumption -- is that you're going to defend and position and spin whatever it is, rather than be part of the process of deciding what is good public relations. And I think at the highest level, that's a misperception but I think your industry has a huge challenge to make it clear that that's a misperception.

JOHN: It certainly is. Harold Burson once said when you accepted the word "communications," though, as a synonym of "public relations," you're sliding on a slippery slope.

TOM: Any comment to that or any other question?

TOM MARTIN: Well, first of all, I'm not one who believes that we should run away from the description "public relations." I think we'd be better off trying to amend the problems that we have, whether it's things that are self created and I would say that a lot of what has happened in the last couple years has been self inflicted and have been problems that we have known were just sort of waiting to happen. Which is if you don't identify spokespersons, if you don't identify the sources of funding for surveys, if you're not transparent in your tactics, then it's just an accident waiting to happen. And I think that's what did happen in some of these cases.

JOHN: Don't you think the credibility of public relations in general suffered a bit when it had absolutely no formal comment on the kiting of bills on the west coast, on the misrepresentation, the money laundering, all of which made legal cases and front page news.

TOM MARTIN: There's no doubt that our profession has suffered from not just that, but a lot of other things that have happened, even things that have happened more recently, as recently as a couple weeks ago with Edelman's issues about ...

JOHN: On the blog business.

TOM MARTIN: Yes. But like I say, I think that's a lot of self inflicted wounds and I think we have to be honest and hold up the mirror and ask ourselves, "Are we behaving in a way that we can defend?"

JOHN: Well, at least the gentleman apologized; I didn't hear that word from the other two CEOs.

TOM MARTIN: Actually Ray Kotcher has. He did that in one of own Page One teleconferences last year.

JOHN: That's all within the family; I'm talking about in public.

TOM MARTIN: Well anyway, I don't want to get into a debate...

TOM: Oh, nicely done ...

JOHN: Well that's the trouble of...

TOM MARTIN: It's arguable that we have suffered...

JOHN: We don't look in the mirror often enough.

TOM MARTIN: That I would agree with.

KIRK: I also would say that, certainly, our industry is not unlike almost every other industry in the sense that we all have our challenges from time to time and I'm not certain that the behaviors of a few should necessarily denigrate the advice and counsel that people in this profession provide to their CEOs daily.

TOM: As we have just a couple of minutes here, I'd just like to go around the table to the three of you on this subject and ask a question. I'll use the term "communications," which has a slightly broader context and a sometimes different one than the term "public relations," which I think Michael so correctly pointed out. In the context of communications, what are the things that all of you see that the profession now does well in trying to stay on top of these kinds of issues that we all need to be aware of doing even more of in the future?

MICHAEL: Well again, I'm the furthest from it, but from what I've seen from the programs I've been part of, I think this is a very self-reflective profession. I think it's asking itself the right questions. I think it's really forcing itself to look at it. I don't know that it's yet come up with the solutions, but I think the willingness of the profession to really examine what it can do better and how to do it better is a critical factor that a lot of professions don't have.

TOM: Okay, Kirk.

KIRK: What was the question again?

TOM: The question is, “What has this issue brought to light, and what are the things that you believe that communications, as a function, is really starting to do well in this context that it should do even more of?”

KIRK: Sure. I guess this is, again, maybe a little hopeful on my part, but I would hope that as a result of all this, the communications people are asking more questions. Particularly about what kinds of policies and procedures and protocol are in place to at least begin to try to hold some people accountable for their behavior. I would say on the response side, I think that hopefully communications executives are having the ability to help organizations maybe be more transparent and more willing to admit where their shortcomings are as opposed to trying to defend the status quo in the face of data that might suggest otherwise.

TOM: Okay, and John?

JOHN: Well, I think that the communications people do a good job when they're asked. The problem is, how do they get to be asked? That means taking risks, taking initiative, having results, having passion. I don't think they fight hard enough to move up the table.

TOM: Okay, so from your point of view, it is do more of that even.

JOHN: Michael, while I've got you on the phone, I want to tell you I've read many of your

papers and I admire your straightforwardness and plain talk.

MICHAEL: Well thank you so much.

JOHN: Non-academic.

MICHAEL: In the land of the blind, the one-eyed man is king.

JOHN: I have two eyes and I can still see it.

TOM: I think with that repartee we will finish here today and I want to thank all three of you very much for participating in a very lively discussion. A lot of great insight over the last hour has come out, so Michael and John and Kirk, thank you very much.

PANEL: You're welcome, thank you.

TOM: And to everybody on the line today, thank you very much for joining us this afternoon. I also want to thank Paul Basista and Susan Chin from the Arthur W. Page Society for putting together this teleconference and making it happen. We thank all of you for joining us today.



ARTHUR W. PAGE SOCIETY

## THE ARTHUR W. PAGE SOCIETY OFFICERS, TRUSTEES AND STAFF

---

### Executive Committee

#### *President*

Roger Bolton

#### *Vice Presidents*

Angela A. Buonocore

Peter D. Debreceeny

Maril Gagen MacDonald

William G. Margaritis

Thomas R. Martin

Anne M. McCarthy

#### *Secretary*

Richard D. Jernstedt

#### *Treasurer*

Nancy A. Hobor

#### *At Large Members*

James E. Murphy

W.D. (Bill) Nielsen

### Trustees

Paul A. Argenti

Catherine V. Babington

Ann H. Barkelew

Roger Bolton

Angela A. Buonocore

Paul Capelli

Peter D. Debreceeny

Valerie Di Maria

Gregory Elliott

Matthew P. Gonring

Kimberley Crews Goode

Harvey W. Greisman

Nancy A. Hobor

Aedhmar Hynes

Richard D. Jernstedt

Raymond L. Kotcher

Thomas J. Kowaleski

Maril Gagen MacDonald

William G. Margaritis

Thomas R. Martin

Anne M. McCarthy

James E. Murphy

W.D. (Bill) Nielsen

James S. O'Rourke IV, Ph.D.

Helen Ostrowski

Ellen Robinson

Kenneth B. Sternad

Joan H. Walker

Donald K. Wright, Ph.D.

### Executive Director

Paul Basista, CAE

### Executive Assistant

Susan S. Chin

### Communications Director

Dawn Hanson

\* As of December 31, 2006



ARTHUR W. PAGE SOCIETY

## 2006 COMMITTEES AND TASK FORCES

---

### President's Council

Roger Bolton, Chair  
Ed Block  
Dave Drobis  
Larry Foster  
Jack Koten  
Marilyn Laurie  
Tom Martin  
Jim Murphy  
Bill Nielsen  
Kurt Stocker

### 2006 Annual Conference Committee

Maril MacDonald, Chair  
Peter Debreceny, Co-Chair  
Catherine V. Babington  
Mark Bain  
Patricia A. Bergeron  
Angela A. Buonocore  
Marguerite F. Copel  
William F. Doescher  
Dominic Fry  
Matthew P. Gonring  
Patricia L. Harden  
Raymond C. Jordan  
Margery Kraus  
Judith A. Mühlberg  
Joan H. Walker

### Business Schools Committee

Jim O'Rourke, Chair  
Matt Gonring, Co-Chair  
Paul Argenti  
Jack Bergen  
Clarke Caywood  
Lou Anne J. Nabhan  
Frank Ovaitt  
James Rubin  
Don W. Stacks  
Ken Sternad

### Executive Committee

Roger Bolton, Chair  
Angela Buonocore  
Peter Debreceny  
Nancy Hobor  
Rich Jernstedt  
Maril Gagen MacDonald  
Bill Margaritis  
Tom Martin  
Anne McCarthy  
Jim Murphy  
Bill Nielsen

### Financial Planning and Operations Committee

Nancy Hobor, Chair

#### *Sub-Committee Leaders*

Bill Margaritis, Non-Dues Revenue  
Ray Jordan, Investments

#### *Other Members*

Kristen Bihary  
Mary Jo Keating  
Bill Nielsen

### Honors Committee

Marilyn Laurie, Chair  
Ann Barkelew  
Larry Foster  
Jack Koten  
Maril MacDonald  
Bill Margaritis  
Tom Martin  
Bill Nielsen

### 2007 Spring Seminar Committee

Ray Kotcher, Chair

*continued, next page*



ARTHUR W. PAGE SOCIETY

## 2006 COMMITTEES AND TASK FORCES

---

### Membership Committee

Angela Buonocore, Chair  
Ann Barkelew  
Barbara Carmichael  
Gregory Elliot  
Matt Gonring  
Don Kirchoffner  
Maril MacDonald  
Anne McCarthy  
Ellen Robinson  
Ken Sternad  
Don Wright

### Nominating Committee

Tom Martin, Chair  
Roger Bolton  
Dave Drobis  
Rich Jernstedt  
Jim O'Rourke  
Ken Sternad

### Programs Committee

Rich Jernstedt, Chair  
Greg Elliott  
Susan Henderson  
Tom Kowaleski  
Ellen Robinson

### 2006 Spring Seminar Committee

Carol Schumacher, Chair  
Ray Kotcher, Co-Chair  
Paul Argenti  
Cathy Babington  
Elizabeth Brooks  
Dan Collins  
Carol Cone  
Ron Culp  
Al Golin  
Aedhmar Hynes  
Rich Jernstedt  
Charlie Perkins  
Donna Reynolds  
Maria Russell  
Simon Walker

### Diversity Task Force

Kimberley Crews Goode, Chair  
Judy VanSlyke Turk, Co-Chair  
Susan Atteridge  
Peter Debreceny  
Valerie Di Maria  
Vicky Shire Dinges  
Mike Fernandez  
Ellen Weaver Hartman  
Chris Hosford  
Kathy Kelly  
Maria Russell  
Don Stacks  
George Stenitzer  
Mary Stutts  
Cynthia Swain  
Charlie Young

### Page Mission Task Force

Valerie Di Maria, Chair  
Jon Iwata, Co-Chair  
Paul Argenti  
Roger Bolton  
Steve Cody  
Peter Debreceny  
Dave Demarest  
Richard Edelman  
Steve Harris  
George Jamison  
Richard Marshall  
Tom Mattia  
Dave Samson  
Johanna Schneider  
Joan Wainwright

### Future Leaders Task Force

Judith Mühlberg, Chair  
Anne McCarthy, Co-Chair  
Paul Argenti  
Ron Culp  
Dave Demarest  
Kimberley Goode  
Steve Harris  
Bill Nielsen



ARTHUR W. PAGE SOCIETY

## 2006 SPONSORS

---

### Diamond (\$10,000 +)

Abbott Laboratories  
*Catherine Babington*

Accenture  
*James Murphy*

FedEx Corporation  
*William Margaritis*

Financial Dynamics

Gagen MacDonald  
*Maril Gagen MacDonald*

International Truck and  
Engine Corporation  
*Gregory Elliott*

Johnson & Johnson  
*Raymond Jordan*

Landor Associates

Nationwide Insurance Companies  
*Jim Simon*

UPS  
*Kenneth Sternad*

Wal-Mart Stores, Inc.  
*Carol Schumacher*

Wieck Media

### Platinum (\$7,500 - 9,999)

Fleishman-Hillard  
*John Onoda*

Rockwell Automation  
*(Matthew Gonring)*

### Gold (\$5,000 - 7,499)

dentsuAmerica  
*Timothy Andree*

Gillette Company  
*(John F. Manfredi)*

Manning Selvage & Lee

MasterCard Worldwide  
*Harvey Greisman*

Porter Novelli  
*Helen Ostrowski*

Prudential Financial, Inc.  
*Robert DeFillippo*

SAP  
*(Anne McCarthy)*

\*Parentheses denote former affiliation.

continued, next page



ARTHUR W. PAGE SOCIETY

## 2006 SPONSORS

---

### Silver (\$2,500 - 4,999)

AOL, Inc.

*John Buckley*

AT&T

*William Oliver*

Roger & Lynne Bolton

Edelman

*Richard Edelman*

Fleishman-Hillard New York

Lawrence Foster

GCI Group

*Jeff Hunt*

General Motors Corporation

*(Thomas Kowaleski)*

Ketchum

*Raymond Kotcher*

Elliot S. Schreiber

Staples

*Paul Capelli*

TIAA-CREF

*Steve Goldstein*

### Bronze (\$1,000 - 2,499)

Best Buy Company, Inc.

*Susan Hoff*

Harold Burson

Freescale

*(Timothy Doke)*

Thomas & Wanda Martin

Northwestern Mutual Foundation

*Brenda Skelton*

Tyco Electronics

*(Charles Young)*

### Friends (\$100 - 999)

Eastman Chemical Company

*Paul Montgomery*

Kimberley Goode

Helen Ostrowski

St. Paul Travelers

*Shane K. Boyd*

\*Parentheses denote former affiliation.

Sponsorships from 1/1/2006 through 12/31/2006



ARTHUR W. PAGE SOCIETY

## PAGE PHILOSOPHY AND PAGE PRINCIPLES

---

### The Page Philosophy

Arthur W. Page viewed public relations as the art of developing, understanding and communicating character—both corporate and individual.

This vision was a natural outgrowth of his belief in humanism and freedom as America's guiding characteristics and as preconditions for capitalism.

The successful corporation, Page believed, must shape its character in concert with the nation's. It must operate in the public interest, manage for the long run and make customer satisfaction its primary goal. He described the dynamic this way:

“Real success, both for big business and the public, lies in large enterprise conducting itself in the public interest and in such a way that the public will give it sufficient freedom to serve effectively.”

### The Page Principles

- *Tell the truth.* Let the public know what's happening and provide an accurate picture of the company's character, ideals and practices.
- *Prove it with action.* Public perception of an organization is determined 90 percent by what it does and 10 percent by what it says.
- *Listen to the customer.* To serve the company well, understand what the public wants and needs. Keep top decision makers and other employees informed about public reaction to company products, policies and practices.

- *Manage for tomorrow.* Anticipate public reaction and eliminate practices that create difficulties. Generate goodwill.
- *Conduct public relations as if the whole company depends on it.* Corporate relations is a management function. No corporate strategy should be implemented without considering its impact on the public. The public relations professional is a policymaker capable of handling a wide range of corporate communications activities.
- *Realize a company's true character is expressed by its people.* The strongest opinions—good or bad—about a company are shaped by the words and deeds of its employees. As a result, every employee—active or retired—is involved with public relations. It is the responsibility of corporate communications to support each employee's capability and desire to be an honest, knowledgeable ambassador to customers, friends, shareowners and public officials.
- *Remain calm, patient and good-humored.* Lay the groundwork for public relations miracles with consistent and reasoned attention to information and contacts. This may be difficult with today's contentious 24-hour news cycles and endless number of watchdog organizations. But when a crisis arises, remember, cool heads communicate best.

**Arthur W. Page Society**

317 Madison Avenue, Suite 2320  
NY, NY 10017  
Phone: 212/400-7959  
Fax: 212/922-9198  
[www.awpagesociety.com](http://www.awpagesociety.com)

Editor: Dawn Hanson  
Design: Catherine Vogel, CVdesign

*Arthur W. Page*

ARTHUR W. PAGE SOCIETY