Web Bugs and the Threat to Online Privacy and Security for Consumers and Businesses

Statements of

Gary E. Clayton
CEO

Dr. Steven B. Lucas
Chief Privacy Officer
Privacy Council, Inc.

Kevin G. Coleman
Former Chief Strategist, Netscape
And Strategic Advisor

Before the Congressional Privacy Caucus

March 1, 2001

Thank you for the opportunity to meet with you today to discuss a technology that poses a very real threat to the online privacy and security of American citizens and businesses. It is a technology that is little understood by most businesses or individuals in the technology industry yet ironically, it is widely used on the Internet today. I am speaking of Web Bugs, which are basically pieces of software than can easily stalk your every move on the Internet without your knowledge. Web Bugs can steal information from your computer hard drives. They can turn on your computer's microphones and record your conversations. They can turn on your computer's video camera and transmit your images to third parties. And all of this can be done without your knowledge and through your computer's security such as firewalls.

My name is Gary Clayton and I am CEO of Privacy Council, Inc. Also here with me today is Dr. Steven B. Lucas, the Chief Privacy Officer of Privacy Council, Inc. Privacy Council, Inc. is a Texas-based company that provides privacy services and technologies to businesses here in the United States and abroad. Also with us today is Mr. Kevin Coleman, the former Chief Strategist of Netscape who is now a strategic advisor for Intelytics, a spin off of iVenturelabs, technology development company based in Pittsburgh, Pennsylvania.

In my job I travel quite a bit. When I check into a hotel, one of the first things I do is to plug in my laptop, dial up the Internet and check my e-mail and other information on the Internet. In order to protect my computer from viruses, I have installed virus protection software as well as a personal firewall that should protect my computer from most intrusions.

As I download e-mails and browse my favorite websites, without my knowledge or consent, I can download Web Bugs. These small pieces of software easily escape detection of my security software because they use the basic functionality of the Internet. In order for a firewall or virus protection software to stop Web Bugs, they would have to keep my computer from downloading any e-mails or any images or Web pages from the Internet. Because this cannot be done without keeping me from using the Internet, I download without knowing if I have downloaded a Web Bug.

In a demonstration to several of your staff members, I turned on my computer, viewed what appeared to be a normal Web page, and immediately infected my computer with a Web Bug. What did it do? Despite the fact that we were looking at my computer screen and monitoring what it was doing, and despite my security software, the Web Bugs installed onto my computer in the Start Up folder. This means that every single time I turn on my

computer, the Web Bug immediately starts. Additionally, the Web Bug made a copy of over 1800 names, phone numbers, addresses and e-mail addresses that I had in my Outlook and sent it to a third party – all without my knowledge and without any indication that this had happened other than a copy of an e-mail left in my "sent" folder of my computer.

This is only a small example of what Web Bugs can do. And they are not just a threat to consumers. Web Bugs can be placed on a company's Web site completely without the company's knowledge or permission. Once the bug is placed on a company's Web site, it can stalk every single customer who visits the Web site, track their every move on the Internet, and send back basically any information that the Web Bug host wants to obtain from the company's customers. It can do all of this without the knowledge and consent of the company, the company's IT department and without the permission or knowledge of the company's customers.

Rather than merely talk about Web Bugs, we are going to show you what they can do. We are going to demonstrate two types of simple Web Bugs and you will see how powerful and insidious they can be. And you will see how completely unprepared we are to protect ourselves against this type of intrusion.

The first Web Bug that we will demonstrate will penetrate my security software, place itself in my computer's Start Up folder and then run every time I turn on my computer. This type of bug could be designed to do basically anything that the Web Bug host wanted, from stealing my contact list or pass words, to making a copy of everything I type or save on my computer and then sending it to the Web Bug host.

The second type of Web Bug that we will demonstrate will silently steal information directly from my computer. This will be done through my security software and without my knowledge. We will have the Web Bug host return the information to us in an e-mail to show how easy it is to take information that each of us considers private or intellectual property.

I am using a new IBM ThinkPad X-20 using the Windows 2000 Professional Edition™ operating system. I am running Microsoft Internet Explorer™ Version 5.50.4522.1800 with all updates and patches as of midnight, February 28, 2001. The computer is protected by Norton SystemWorks 2001™ with the latest virus protection updates and by the e-mail, real time e-mail scanning and protection fully enabled. Again, the updates are current as of midnight February 28, 2001.

Before I begin, I want to show you my computer's Start Up folder that contains those programs that my computer will automatically start when I turn on the computer. As you can see, there are only a limited number of folders and nothing entitled "Start" which is what the Web Bug folder will be called when it is placed on my computer.

I am dialing to my Internet Service Provider through AT&T Global Network using a Washington, D.C. local dial-up connection and an analog line. Once I am connected, I will go to a site on the Internet that has the first type of Web Bug that will be installed on my computer. This site has been created by Intelytics and you will see that there is no notice or disclosure of neither what will happen nor anything that alerts us to the fact that the Web Bug will be installed. In addition, there is no opportunity for me to consent or even "opt-out" of having the Web Bug placed silently on my hard drive and in my Start Up folder.

What you do not know is that while we were simply looking at the Web page, the Web Bug has already been placed and has infected my computer. Even if the site had contained a privacy notice to tell me that such a bug was about to be placed on my computer, it would be too late. Why? Because the Web Bugs infected my computer from the very second I downloaded the page.

I am now going to show you my computer's Start Up folder again. You will notice that there is a new folder there that is labeled "Start." When I click on the folder, or when I simply turn on my computer again, this Web Bug will start. This particular Web Bug has been designed to simply present us with a notice that warns us that the computer has now been infected. The notice states:

> *"Hi. A Web Bug has now infected your computer. We just put this on your computer so that it will run every time you start your computer. We can make this Bug do just about anything we want. For example, we told it to steal your Outlook address list and send it to us via an e-mail. Every single time you turn on your computer, it will send us an updated list of your contacts and the personal information contained on their contact forms. AND, it will happen without your knowledge or permission. Have a nice day."*

It could have been designed to steal any information from my hard drive or to track my every move on the Internet and then report that information back to the Web Bug host. It could have easily stolen my personal budget or tax information files. Or it could have stolen my

company's patent application. Or even the entire contents of the files on my computer.

Let me show you how easy this can be done.

Immediately prior to this demonstration, I was sent a Excel file from one of your staff members. I opened the file immediately prior to coming into this room and simply stored it on my computer's C drive in a folder that was named by your staff member. Neither I nor anyone else with Privacy Council or Intelytics had seen the contents of the file.

I am now going back onto the Internet to what appears to be a normal Web site that has been prepared by Intelytics. Again, this site has been designed with a Web Bug for use in the demonstration. As the page is loaded onto my computer, it is again infected without my knowledge. And without being detected by my security software.

This particular Web Bug has been designed to send a list of the files on my hard drive back to the Web Bug host. As you can see, there is nothing that happens that would alert us to what is being copied nor even to the fact that the Web Bug has stolen my files.

Intelytics is now going to send us the name of the Excel file that your staff member prepared. And they will send us a copy of the file attached to an e-mail. This e-mail will appear in my Outlook. This happens in an instant. While I was talking and while the page was loading, the Web Bug was sent from Pittsburgh to Washington, D.C. to my computer. The Web Bug then transmitted the information to Pittsburgh where Intelytics viewed a copy of the files. They then simply selected the file they wanted and had that file sent by my computer to Pittsburgh. Again, without our knowledge and without any indication of what was happening.

Here is the e-mail that I have just received. Again, here is the Excel file attached to the e-mail. And, as I open the file that was sent to me, you can see that it is the same file that was just handed to us by your staff member before our testimony today.

This is what can happen over a dial-up modem, on a sophisticated computer with considerably more protection than most Internet users have. With a faster connection, considerably more information could have been stolen. The Web Bug could have been programmed to turn on an attached microphone and store our conversations and then send it to the Web Bug host at a time convenient to the Web Bug host. Or, it could have been instructed to turn on any video camera attached to the computer and then

record what it sees. Again, this information could easily be sent to the Web Bug host.

Or, the Web Bugs could monitor when I visit a site on Diabetes, track my visit, steal my contact information and other personally identifiable information and then send it to the company or to any third party that has placed the Web Bug on the site. It could have been placed on the Web site of a financial institution and be designed to steal PIN or other password and financial information. Or it could be designed to simply notify the Web site operator of the time and date that I visited the site or opened an e-mail. Or notify the Web site operator of the e-mail address and contents of any friend that I send the e-mail.

How Prevalent Are Web Bugs?

During the recent Christmas season, Intelytics conducted a scan of 51 million Web pages. This scan revealed over 15 million of what has been classified as "Type-2" bugs and over 94,000 "Type-3" bugs. Many sites had multiple bugs placed on a single page. On one Web site, a single page had over thirty Web bugs.

Who Uses Them? And Why?

It appears that Web Bugs are currently being used primarily by Internet advertisers. They are being used to track information of sites visited and to provide specific information on the date and time certain information is viewed on the Internet. They are also being used to track when information is forwarded to third parties and when they view and forward the information.

Why? Because this type of information enables advertisers to target individuals with information and to learn about who is really interested in an advertisement or in the contents of an e-mail. They provide information that enables advertisers to discern considerable information about individuals who visit a particular site or who read certain types of e-mails or information.

They can just as easily be designed to learn who is visiting a competitor's Web site or to provide notice of what was ordered and by whom. Or they can be used to track log-on names and pass words. They can copy credit card numbers or other personal information that is sensitive.

Most of this is done without any notice to the Internet user. A survey of Website privacy policies will quickly reveal that very few mention Web Bugs or provide notice that such technology is being used to track an individual. Our experience to date has shown that such bugs are often

placed on a company's Web site without the company's knowledge or permission.

What Are the Specific Types of Web Bugs?

Web Bugs are software applications that can secretly follow online users and report their every move back to the web bug host. At the present time Intelytics has identified at least five types of Web Bugs:

- Level 1 (pixel tags or 1x1 gifs)
- Level 2a
- Level 2b
- Level 3
- Level 4

Each of these web bugs has differing characteristics but all serve as digital cyber stalkers that can watch our every move. To the user, the technology in question is seemingly innocuous. The bugs can open a new window of surveillance on a traditionally private sphere of communications. More troubling, is that the same technology can be used to match a recipient's e-mail address with previously anonymous records of the Web sites visited from that person's computer.

To better understand, discover, and assess the impact of Web Bugs, Intelytics has developed a taxonomy that may be helpful. This categorization may not be exhaustive and is likely to be extended in the future if new types not fitting these criteria are found or hypothesized. The categories are based on manner of infection, location of infection, co-operation of the user, and co-operation of the web site on which browsing information is being collected. We will give details of each of these aspects and a preliminary analysis of what information can be gained from each.

Type 1 Web Bug

This is the classic Web Bug. It is based entirely on the steps taken in the parsing of HTML, the basic scripting language used on the Internet. Originally designed to help match site page requests with a particular user session, it performs this function well. The Bug is implemented by an object (typically an image) that is requested and obtained via an "HTTP GET"

query. What this means is that when your computer logs onto the Internet and downloads the basic information necessary to display a Web page, it can also download the Web Bug. The bug can include additional information in the query string that your computer uses to download the Web page. In the HTTP response, this object sets a cookie on the user's machine that is sent back along with any subsequent HTTP requests to the same Internet domain. The only such bugs that we are concerned with are those that are designed to send information to a site that is different than that where the bug was obtained.

The image tag is not the only manner in which to create Type 1 Web Bugs, merely the most commonly known. The following table lists the possible and known attributes and tags in HTML that can be the source of Type 1 web bugs.

TAG	ATTRIBUTE
APPLET	CODEBASE
BODY	BACKGROUND
EMBED	SRC
FRAME	SRC
IFRAME	SRC
ILAYER	BACKGROUND
	SRC
IMG	DYNSRC
	LOWSRC
	SRC
	USEMAP
INPUT TYPE=IMAGE	SRC
	USEMAP
LAYER	BACKGROUND
	SRC
LINK	HREF
OBJECT	CLASSID
	CODEBASE
	DATA
	USEMAP
	NAME
SCRIPT	SRC
TABLE	BACKGROUND
TD	BACKGROUND
TH	BACKGROUND
TR	BACKGROUND

Type 2 Web Bugs

The second major type of web bug is a Type 2, or system resident, Web Bug. This type of bug works at the operating system or stand-alone application level. This Web Bug infects a user's computer via an executable application that has access to implant the Web Bug on the system. (This can be accomplished during almost any download) The application can monitor network (Web) traffic, cache the information, and relay it to a central repository in batches. The Internet user or site that is being monitored does not have to cooperate since the user has absolutely no knowledge or control of the monitoring.

Type 2 Web Bugs fall into three categories:

•**Type 2a Web Bugs:** This type of bug requires the explicit co-operation, but not knowledge, of the user. In order for the bug to work, the individual must perform some action, such as executing a program or installing an ActiveX component. The user, however, is not aware that this action is allowing a Web Bug to be installed on his or her machine. This type of bug can be seen as a Trojan horse since the monitoring and reporting function is not a stated nor known by the individual.

•**Type 2b Web Bugs:** These do not require the explicit co-operation of the user. These are perhaps the most insidious because they do not require co-operation of either the user or the Web site being monitored in order for them to work. Such bugs can be installed on a computer simply by the process of viewing Web sites or downloading e-mails.

•**Type 2c Web Bugs:** These require the co-operation of the user, but inform the user of their operation. That is, this activity of the Web Bug is a stated functionality of the software that the user is asked to install. In behavior, these are identical to Type 2a web bugs, but differ in the key point that they inform the user.

•**Type 3 Web Bugs:** This type of Web Bug are browser or application resident Web Bugs. These are installed into or directly affect the user's Internet Web browser or other application used to generate and receive HTTP requests. This is the fundamental difference from Type 2 Web Bugs. Like Type 2 Web Bugs, they result from something that the user has downloaded in the course of simply going onto the Internet. Type 3 bus do not require the co-operation of the user to be effective. Further, Type 3 Web Bugs can store their information and relay it in batches to a central place.

They are differentiated into three classes based on the user's knowledge and co-operation:

- **Type 3a Web Bugs:** These require the co-operation but not knowledge of the user.

- **Type 3b Web Bugs:** Type 3b Web Bugs require neither the knowledge nor cooperation of the individual in order to work.

- **Type 3c Web Bugs:** Type 3c Web Bugs require the co-operation of the user but give full disclosure. An example of a Type 3a Web Bug would be a browser plug-in that also monitors and reports a user's browsing information. An example of a Type 3b Web Bug would be some JavaScript (ECMAScript) that exists in another part of a frameset or another window that collects information about browsing. A Type 3c Web Bug is identical to a Type 3a Web Bug in functionality but discloses to the user its web bug nature.

- **Type 4 Web Bug:** The Type 4 Web Bug is a document tracking device that is commonly used in the transmission and tracking of e-mails and attachments. Marketing companies now regularly keep tabs on which prospective customers open e-mail solicitations and when the e-mails were opened. Type 4 bugs allow an advertiser to track message and any related attachments as they are sent to a prospective customer. The advertiser can then identify exactly when the e-mail was received, when it was received and if it was opened. Type 4 bugs can then let the advertiser know when and if the e-mail or attachment was it was sent or even if it was printed or forwarded or electronically copied. This can be done without the individual's knowledge or consent. Further, if the Type 4 bug is forwarded, the new recipient's information can be taken and sent back to the Web Bug host. This can continue as the e-mail or attachment is forwarded or distributed to friends or associates.

With this type of bug, the instant an e-mail is opened, the bug can instruct the computer to display a graphic file. The individual's computer then automatically fetches the image from a specified location on the Internet. By adding a unique identifying code to those instructions, an advertiser can record when a particular recipient retrieves the image, and, thus, when the e-mail message is opened. It is estimated that over half of all Internet users have e-mail software that is susceptible to this type of Web Bug. These types of bugs are also used outside of the United States. For example, Soobok Lee, the founder of Postel Services, a Korean company, recently stated that about 30,000 people had used the company's service since its

introduction in May. Additionally, Soobok Lee stated that several companies that had purchased licenses to track all of their correspondence.

Another practice, which involves using e-mail as a kind of Trojan horse to deliver a cookie file, recently prompted the Michigan attorney general's office to warn that it would sue one Web site, Evite, under the state's Consumer Protection Act unless it began to inform consumers of the practice.

The Implications

Web Bugs and similar technologies represent a growing and sophisticated threat to the privacy and security of consumers, employees, businesses and governments. The very ease of their use and their ability to take information directly from a user's computer hard drive – without detection – pose a serious threat that must be dealt with. Increased use of this type of technology will certainly further erode consumer confidence in on-line transactions. It will also pose serious risks for businesses and governments and confidential and secret information can be easily and secretively obtained. As demonstrated in today's hearing, the ability to pull information directly from a computer can penetrate even into the computers used by Congress, staff and government and judicial officials.

Use of the Web Bug technologies also threatens to have a negative impact on the United States' agreements with other nations. For example, agreements such as the European Union Safe Harbor Agreement could be in jeopardy if businesses in the United States do not act responsibly. The Government of the United States has already recognized and addressed these privacy concerns in June 2000, when the White House instructed the Drug Policy Office to stop using Web Bugs on the government's anti-drug site.

Perhaps the biggest threat arises not from business or governments, but from the use of Web Bug technologies by fraudsters and organized criminals acting within and outside of the United States. The ability to stalk and take computer information will certainly prove to be an attractive and potentially lucrative attraction for criminals.

Congress and the Federal Trade Commission have provided a grace period for online companies to demonstrate their commitment to widely accepted fair information practices. Businesses will certainly argue that Web Bug technology can provide consumers with new products and services. This is undoubtedly true. But the wide spread use of this type of technology also threatens to erode the very public confidence that will be essential for

the continued development and deployment of new products and services on the Internet. The technology threatens the extension of online services that entail confidential or sensitive personal information. This threat is real, serious and it must be addressed.

We believe that law should prohibit the use of Web Bug technology.

PRIVACY COUNCIL™

Privacy Council, Inc. provides businesses worldwide with privacy solutions services. Founded in early 1998 and based in Dallas, TX, Privacy Council advises many Fortune 500 companies, the financial services industry and large and mid-sized Internet companies on transforming their privacy risks into privacy assets. Privacy Council assesses privacy liabilities and offers its clients timely and efficient tools to manage them.

In 2000, Privacy Council, in conjunction with Deloitte & Touche, developed a privacy assessment programs that will be licensed to companies and professionals. The assessment modules provide management teams with the latest privacy information and tools to ensure compliance with worldwide privacy regulation.

Privacy Council has recently developed a patent pending service called Virtual Privacy Officer (VPO) for the financial services industry. The VPO package is a suite a services featuring software solutions to help businesses meet specific compliance concerns of the Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act. In addition, VPO offers a series of self-assessment privacy tools, advanced consulting services, web-based training tools, and industry specific publications.

Privacy Council believes privacy, like security, is a process. It involves an understanding of data flows within an organization. And most of all, it requires different perspectives on how data is and should be used. These perspectives include international, legal, cultural and political, each with its own unique understanding of technology, databases, and security.

Privacy Council provides its clients with a unique blend of talents and perspectives. The result of this multi-disciplined approach helps our clients meet the present and future challenges of today's global marketplace.

PRIVACY COUNCIL™

Gary Clayton is the founder and CEO of Privacy Council. An attorney with over two decades of litigation and commercial experience, Mr. Clayton has been actively involved with the Internet and technology issues since 1994.

He has testified before the U.S. Congress and advised congressional leaders and numerous Members of Congress on privacy and electronic commerce issues. He has also appeared in national and international publications as well as national news programs.

Internationally, Mr. Clayton had spent seven years in Europe and has worked with senior executives of over one hundred multinational companies in London, Geneva, Zurich, Madrid, and Hong Kong on privacy issues and their implications for business.

Mr. Clayton has brought together Privacy Council a team of experts with many years of experience in network architecture and security, telecommunications, databases, financial institutions and international data protection.

Mr. Clayton received his M.A. from the School of International Service, American University, Washington, D.C. and his L.L.M. in European and International Business Law from the University of Exeter, England. He received his B.S. and J.D. degrees from Louisiana State University. He has also attended law courses at the Universit de St. Domaine, Grenoble, France.

PRIVACY COUNCIL™

Dr. Steven Lucas brings over 18 years privacy experience in the information technology industry to Privacy Council where he oversees client consulting services for the company. Dr. Lucas is an expert in the areas of privacy law, e-commerce, public policy, computer security, database marketing, and database technology.

Dr. Lucas has been responsible for leading several leading companies efforts in legislative and standards development and providing both technical and legal insight towards the company s privacy and electronic commerce objectives.

Dr. Lucas has established relationships with key decision-makers through his involvement in leading organizations. He is on the Board of Directors for TRUSTe, the United States Internet Industry Association, and the Personalization Consortium. He is also a member of the U.S. Ecommerce Committee, the Trans Atlantic Business Dialogue (TABD), the Online Privacy Alliance, Computer Security Institute, International Computer Security Institute, International Data Warehouse Association, Internet Society, the Institute for Electronics and Electrical Engineers (IEEE), and the International Security, Privacy, and Trust Association. Dr. Lucas was also recently appointed by the Governor of Colorado to the Information Technology Advisory Board where he will lead the State of Colorado s effort s to establish privacy laws for both the public and private sector.

Considered an expert in privacy law, e-commerce, computer security, database marketing and database technology, Dr. Lucas frequently speaks at industry events, often presents to the Department of Commerce and the Federal Trade Commission and is a member of the Presidential Summit Planning Committee. He has also appeared before the European Union Commission and participated in the meetings between the United States and Europe as a member of the Department of Commerce delegation.

Dr. Lucas has appeared in all types of media. He was featured on CNN and MSNBC. He has been featured in CIO and ComputerWorld magazines. He has been quoted by every major publication including the Wall Street Journal, New York Times, Business Week, San Jose Mercury News, Wired, InfoWorld, Federal Computer News, National Journal of Technology, Legal Times, and the Denver Post. He has presented at several International conferences as an invited expert on International privacy law. He is a fellow of the International Computer and Law Institute.

Dr. Lucas has assumed a leadership role in the development of technology and standards for privacy and ecommerce. His activities have included being the Editor of the Protocols and Data Transport Working Group on the Platform for Privacy Preferences Project (P3P) and the Chair of the Syntax and Encoding Group of P3P

within the World Wide Web Consortium (W3C). Dr. Lucas is also the Co-Chair of the IEEE Internet Best Practices Working Group and maintains advisory roles within the Direct Marketing Association, Internet Engineering Task Force, Internet Advertising Bureau, and the Web Accessibility Initiative within the W3C.

Dr. Lucas was the Senior Vice President, Chief Information Officer, and Chief Privacy Officer of Persona and President of Persona s Privaseek consulting and technology division. He was a member of the original launch team for both companies. At both Persona and Privaseek, Dr. Lucas was responsible for leading the company s efforts in legislative and standards development and providing both technical and legal insight towards the company s privacy and electronic commerce objectives. He was responsible for ensuring that both companies maintained a leadership role in the consumer privacy space. He was also responsible for all engineering functions and managed a multi-million dollar I.T. budget.

Prior to joining PrivaSeek, Dr. Lucas was Chief Information Officer for Excite@Home's MatchLogic division, where he provided counsel and oversaw monitoring of legislation and lead MatchLogic s technology standards activity. Before MatchLogic, Dr. Lucas was the Chief Technologist and Senior Principal Consultant for dbINTELLECT Technologies. In this position, Dr. Lucas managed major accounts for EDS, Dun and Bradstreet, AC Nielsen and The New York Times. In this capacity, he was responsible for the design and implementation of some of the largest direct marketing databases ever created. Dr. Lucas has also held positions with Neodata Services, one of the worlds largest direct marketing organizations as the Chief Technology Officer where he was responsible for all aspects of the design of one of the largest database marketing systems ever built and the migration of several terabytes of data from legacy systems to supercomputers and Unix systems. He also held positions at EDS as a Consultant Systems Engineer, and Bell Labs as a member of technical staff, where he participated in the development of the UNIX operating system.

Dr. Lucas received his Ph.D. in Computer Science from Stanford University. He also received a B.S. in Electrical Engineering from The Citadel, an M.B.A. from New Hampshire College, and a J.D from the American College of Law.

Kevin G. Coleman

Kevin G. Coleman is a seasoned technology executive with nearly two decades of experience. Since the inception of eCommerce and eBusiness, Kevin G. Coleman has been a significant force behind the Internet revolution to transform global business. His accomplishments stand out among the leaders in his industry and he has helped to write the rules of doing business in the new economy. Mark Andreessen, co-founder of Netscape called him, "One of Netscape s most creative thought leaders". Mr. Coleman is a sought after source of insights and information about today s fast-paced business & technology environments and has participated in more than forty interviews and published more than a dozen white papers. Currently, Mr. Coleman is using his research and experience to pioneer Compete-21 Strategies for Success in the Global Digital Economy (http://www.compete-21.com/)

With nearly two decades of business experience and advanced academic credentials in Business & Technology, Mr. Coleman brings with him a unique perspective on management, technology and the global business environment. He was the Chief Strategist for Netscape, the quintessential Silicon Valley success story, and has worked for leading consulting organizations such as Deloitte & Touch and with CSC Consulting in the Reengineering Practice. During his career, he has consulted in more than a dozen countries and almost thirty states. Working with the leaders of some of the world s largest and most prestigious companies, Mr. Coleman has assisted organizations in achieving breakthrough performance by leveraging new technology to change the way business is conducted. He has personally briefed executives from 15 of the 50 largest companies in the world and nearly 500 CEOs worldwide. He is a strategic advisor to multiple companies and holds several board positions, including a board seat for the National Technology Transfer Center (NTTC), the organization responsible for commercialization of all government sponsored research.

Mr. Coleman routinely lectures and speaks on an international level covering such topics as management, strategy and technology, as they relate to the global business environment. He has also lectured at many of the world s largest and most renowned educational institutions bringing the realism of global business into the programs of our universities. He has published numerous articles in business and trade publications and authored multiple chapters in the "Encyclopedia of Computer Science and Technology", including one on Strategic Planning, as well as co-authored the book: Reengineering MIS. While at Netscape he has authored numerous executive briefs, including Strategies for Success in the New Economy, Financial Services in the Net Economy, Telecommunications in the Net Economy and Strategic Alliances. Executive briefs entitled The 21st Century CEO and Technology and the 21st Century Business will be released shortly.

Three US. Patents, three Excellence in Design Awards from Design News, two Product Development Awards from Dravo Corporation and the 1991 Bronze IDEA Award from Business Week are evidence of Mr. Coleman s unique combination of business and technical expertise. Most recently he has been named as an honored member of Who's Who in the Computer Industry and as a lifetime member of Who's Who in Business Worldwide: Platinum edition. In addition, he has been recognized in the 16th Edition of Men of Achievement and received the 1993 Citation of Meritorious Achievement. Mr. Coleman was also a nominee for the 1998 Presidential Medal for Technology.