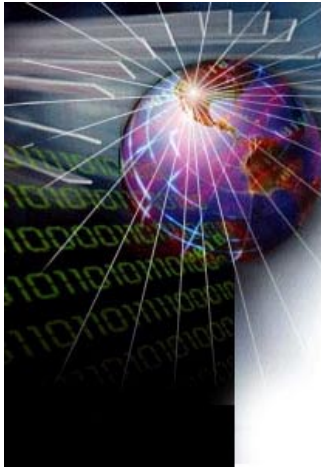


Reprinted by TradeHarbor with Special Permission from Strategic News Service



Strategic News Service

The **Strategic News Service**[®] is the most accurate predictive newsletter covering the computing and communications industries.

It is read by top management and financial analysts in these industries worldwide.

This service is intended for strategic thinkers who depend upon business technology planning.

The SNS charter is to provide managers with information that is not available in the press about critical computer and telecommunications issues, trends and events.

www.stratnews.com

www.stratnews.com

SUBSCRIBER EDITION

STRATEGIC NEWS SERVICE[®]

"Next Year's News This Week"

*The most accurate predictive letter in computing and telecommunications
Read by industry leaders worldwide*

This May 13th, 2003 Issue:

*****SNS*** SPECIAL LETTER: BIOMETRICS: NEXT YEAR'S HOT TECHNOLOGY?**

Provided by: Technology Alliance Partners

On the Web: <http://www.tapsns.com>

TO SUBSCRIBE, EMAIL SNS@TAPSNS.COM WITH THE WORD "SUBSCRIBE" IN YOUR MESSAGE; YOU WILL BE BILLED LATER (see the end of this newsletter for details).

RE-SENDING OF THIS NEWSLETTER TO ANY NUMBER OF COLLEAGUES IS ENCOURAGED ON A ONCE-PER-USER BASIS, PROVIDED YOU ALSO CC: SNS@TAPSNS.COM; IN RETURN, WE WILL PROVIDE RECIPIENTS WITH A ONE-MONTH FREE TRIAL SUBSCRIPTION.

Not for Public Distribution

ANY OTHER UNAUTHORIZED REDISTRIBUTION IS A VIOLATION OF COPYRIGHT LAW.

This May 13th, 2003 Issue:

*****SNS*** Special Letter: Biometrics: Next Year's Hot Technology?**

By Bob Nelson

The FIRE Box: Updates On The SNS Future In Review 2003 Conference

What is it: The SNS FIRE Conference will provide a 3-5 year global technology markets outlook, based on discussions with internationally-recognized leaders in technology, economics, equity markets, and politics. If you are a senior executive or investor whose business depends upon the future of technology markets, you should join us at the Hotel del Coronado from May 19-22. (Add a few days and make it a family vacation). For more information, go to <http://www.futureinreview.com>, or contact Sharon at sam@tapsns.com.

What's New: FIRE attendees will love this one! Andreas Bechtolsheim, current Tech VP at Cisco, and past co-founder of SUN and Granite Systems, is joining our Future of Computing Panel. Yes, that would be Michael Dell, Ray Ozzie, Pat Gelsinger and Andy, all discussing where computing will be in five years. And no, it isn't too late to sign up, but you'll have to resign yourself to getting your totally cool embroidered SNS FIRE laptop case after you return home.

We will also see a demo of Authora's new encrypted business transaction platform (in the Modviz breakout), and a demo of Ndiyo's new computer prototype for the Rest of the World (in the Project Inkwell breakout).

Who's Attending: An ongoing roster, for those who have yet to visit the website, of speakers and those participants already signed up. We are happy to welcome the following attendees to FIRE 2003: Steve Waite, Partner and Chief Knowledge Officer, The InfoPro, NYC; Bruce Wilcox, VP of eBusiness, Harcourt Education, Orlando; Lee Brillhart, Chairman and CEO, Survival, Inc.; Craig Cline, VP Content, Key3Media; Roman V. Dijour, VP, Warburg Pincus; Spencer Hyman, Managing Director, Copan UK; and many more.

I would also like to give a special note of gratitude to **Warburg Pincus** for becoming a FIRE Gold Level Sponsor.

Publisher's Note: Next week there will be no SNS issue, as all of our cycles will be dedicated to the FIRE Conference. I am looking forward to the many meetings of SNSers who have become e-friends going back as far as 1995, but for whom this will be the first chance to meet in person.

Not long ago, Bob Nelson wrote to me and began to make his case for voice authentication as a breakthrough of sorts, less from a technical perspective than from the view that the timing was right, and the technology fit the requirements of the marketplace. After all of the discussion we've had in these pages about using voice recognition on a more advanced plane, Bob's arguments seemed to make sense.

As with The Year of the LAN (which lasted a decade at least), the title of Bob's piece this week is unimportant: whether he's right in general is very important. Let's see what you decide. – mra

*****SNS*** SPECIAL LETTER: BIOMETRICS: NEXT YEAR'S HOT TECHNOLOGY?**

By Bob Nelson

Have you ever called the customer service number for one of your financial services providers, entered your account number and social security number, and then stopped to think that identity thieves could easily obtain that same information and gain access to your financial accounts?

On the same call, when asked "What is your mother's maiden name?" has it crossed your mind that the customer service company has thousands of employees with full access to the secret answers you have shared to help validate that it is really you calling?

If the above issues concern you, you now know why for the last several years biometrics has regularly been touted as Next Year's Hot Technology, even though it has yet to take off. In a recent exchange of emails on the subject with Mark Anderson, he proposed that I share some thoughts on why, this time, biometrics might really be the Hot Technology For 2004, how the first consumer biometrics might start to roll out, and the opportunities biometrics presents for SNS readers and 6 billion other people.

A Little Background

"Biometrics," for our purposes, refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, among others.

The allure of biometrics is based on its potential to help businesses and individuals authenticate *who you are* in contrast to *who you say you are*. With identity theft in the United States alone affecting up to 700,000 people a year and causing the financial services industry losses of an estimated \$4 billion a year and growing, the ability to truly authenticate individual identities has for many years suggested a bright future for biometrics.

To date, most authentications have been based on *what you have*, such as an ATM card, credit card, driver's license with a picture, or other identifications that are issued to you by sponsoring institutions. Another level of what you have includes technologies such as public key encryption that are issued by "certificate authorities" and identify a specific computer or device with a token that authenticates not you but a registered item of yours. The next level of security for authentications is *what you know*, such as your Social Security number, your ATM card PIN number, your password for a financial services

website, or a shared secret such as your mother's maiden name for transacting with your bank's toll-free call center.

The promise of biometrics is that items or information that can be stolen, forged (your credit card or driver's license), or obtained through fraudulent means (your Social Security number, mother's maiden name, or birth date) could no longer be used by one person to impersonate the identity of another, reducing or eliminating the havoc that identity thieves can wreak upon the lives and financial welfare of their victims. Since they are part of *who you are*, personal biometrics are highly resistant to being stolen or compromised.

Why then the long delay in adoption, if there is a presumed pent-up demand for next-generation authentication technologies? One of the key unresolved factors has been the nature and extent of biometrics registries – databases containing the biometrics of millions of individuals. How should these databases be built? How should they be used? Who should have access and who should not?

The nascent biometrics industry is rapidly approaching key decision points in each of these areas that will set the stage for the release and rapid acceptance of new biometric technologies. Let's look at how biometrics might actually work.

Selecting An Initial Biometric

Suppose you represent a Fortune 500 company and you want to build a registry of biometrics for your customers to resolve authentication requests quickly and accurately. Your first exercise will be to determine which biometric would be most effective in gaining the enrollments of tens of millions of consumers. As you research the most common options – eye, hand, face, finger, or voice – you are likely to be struck by one overriding consideration. If you want to register millions of consumers by eye, hand, face, or finger, you will need to buy and deploy tens or hundreds of thousands of "reader devices" and then induce consumers to come to your enrollment centers, bring required supporting identification, and then enroll with the help of your staff. Then, once you gained the enrollments, the only time you could authenticate the enrollees would be at locations where compatible readers were installed and networked.

That leaves you with voice as the only biometric that allows for remote enrollment, since consumers can register using any telephone, anywhere, anytime. Having eliminated the cost of buying and deploying thousands of reader devices and the necessity of finding clever ways of incenting millions of consumers to physically visit your enrollment centers, you now have the question of how to get millions of consumers to call to register their voices in a biometric registry. So you create a list of the 20 or 30 industries in the United States (to start) that have companies with customer bases of at least 5 million consumers. You might rank those industries based on the following criteria: 1) How much trust do consumers have in the companies representing that industry? 2) Does the customer relationship provide enough profit to support the costs of enrolling millions of voice biometrics? 3) Are the net savings to the industry large enough to induce them to support and integrate a brand-new technology?

As you wend your way through industry analyses and consumer research, you might conclude that the industry that consumers are most likely to trust to enroll, store, and manage their personal biometrics are financial services providers, as they are built on a legacy of fiduciary trust. You would next look at the

many types of financial services providers to establish the optimal point in the customer relationship for the company to request or require enrollment in a voice biometric system – and you might have another AHA! moment. What about at the time your credit card company mails you a new or renewed card, requiring that you "activate" the card by calling a toll-free number from your home telephone and touchtone entering (or, nowadays, perhaps voicing) your account number, your Social Security number, or other personal information. If the bank is willing to extend \$1,000 to \$25,000 of credit just based on a call from your home telephone number and a few digits, wouldn't it be possible to ask the caller to enroll in the new service to help them guard against identity theft and credit card fraudsters?

A Real-World Test

The Financial Services Technology Consortium (<http://www.fstc.org/about/institutions.cfm>) is an industry research organization funded by 16 of the largest financial institutions in the United States. Its charter is to trial early-stage technologies that have important potential for the member organizations as a means of sharing the cost and effort of piloting new technologies. Recently, the FSTC completed a four-month Voice Authentication Study (<http://www.fstc.org/press/030326.cfm>) in conjunction with an industry-leading user interface research firm, TouchPoint Consulting, that focused on both consumer acceptance and vendor implementations. While the results of the study are reserved for project sponsors, one can infer the potential interest in voice authentication from the list of 10 corporate sponsors, which includes Dreyfus, JPMorgan Chase, Merrill Lynch, VISA, and Wells Fargo.

The goals of the FSTC Voice Authentication Study were determined by the project sponsors and were divided into two phases. Phase I was focused on consumer research to study customer attitudes, preferences, and potential facilitators or barriers to enrollment and use. Phase II consisted of in-depth individual consumer interviews that featured hands-on usability testing of systems provided by contributing technology vendors. Together, the sponsoring organizations gained an understanding of consumer willingness to enroll in voice authentication systems and to be authenticated by them. In addition, they learned that consumers appreciated financial services providers that would offer voice authentication services to their customers as a way of reducing fraud for the banks, since it also reduced the possibility that the consumer would suffer from identity theft.

The primary benefits perceived by consumers in the FSTC study were that their bank accounts could not be accessed or manipulated by anyone but themselves using voice authentication, and that identity thieves could not order products from direct merchants (such as Dell or LL Bean) by providing a fraudulently obtained credit card number from an unsuspecting cardholder if the merchant required a "voice signature" on the telephone and, in the future, in Internet sales transactions. One of the primary findings from the study was that, with proper preliminary information provided by mail, web, or phone script, it is likely that 80 to 90 percent of consumers or more would be willing to enroll in a voice biometric service offered by major financial services providers.

Voice Biometrics For Consumers

Throughout the 1990s, it had been assumed within the small universe of biometrics companies and their analysts that a mass consumer rollout for biometric enrollments and authentications might never get off the ground due to overwhelming objections from the public, government agencies, or consumer privacy organizations. Since 9/11, however, it appears there has been a fundamental shift in thinking by

consumers who now may well value personal security much more highly than personal privacy. If that is indeed the case (I leave it to the market research and analyst communities to objectively quantify such a shift in consumer behaviors and beliefs), then the preconditions for companies to offer biometric authentication services may, for the first time, provide for business models that presume overall acceptance and large-scale adoption.

There are two primary ways, then, that mass consumer voice biometrics might evolve in the marketplace:

Multiple Enrollments – Consumers are asked to enroll at each institution they do business with. If each company that has a need to enroll and authenticate customers asks you to enroll, and then keeps that enrollment for its exclusive use, consumers potentially end up enrolling with their checking account provider, their credit card provider, their insurance provider, their mortgage company, etc., etc. Under that model, consumers have to make a yes/no decision to register with each vendor that requests their enrollment. This is similar to all of the passwords needed today for different e-commerce sites on the Internet. A variant of this model allows you to set up a single webpage and then register all of your passwords once so you can access all your preferred e-commerce sites from your Start page. This account aggregation service was pioneered by Yodlee and is now offered by many top banks, in part so they can gain a view of the many business relationships you maintain.

Single Federated Enrollment – Consumers are asked to enroll directly with a single company that then shares the enrollment with authorized vendors which, presumably, have been screened for trustworthiness. This model is similar to Microsoft Passport or the Liberty Alliance in the online world, which enroll your identity information once and then share it with numerous e-commerce sites that link back to your original enrollment when you request it. For the consumer, the promise is enroll once, and use that authentication technique at numerous sites on the Internet. For businesses, the goal is to simplify the sales process by requiring a minimal amount of information to access the visitor's original enrollment data. A variant of this model is Verified by VISA and MasterCard SecureCode, in which you register once with your issuing credit card company and then, when you transact with any affiliated merchant, you merely type your chosen private code number so the merchant can authenticate against your enrollment.

While on the surface it would seem that consumers might not mind enrolling their voices with numerous companies they already do business with, in reality, are you and 290MM US citizens likely to be comfortable leaving a biometric identifier with two, five, or twenty different companies over time? It's doubtful – particularly if some of the requesting companies are not businesses with which you have an existing financial relationship but are instead new or small companies with whom you are a first-time customer. When you consider that these companies could then end up being acquired by other companies that don't have the same regard for the privacy assurances that were originally provided to you, your willingness to enroll might be seriously diminished.

A counterintuitive thought is that consumers may actually be comforted by knowing that they will be asked to enroll only once by a company with which they have developed a trusted relationship, and that company will be responsible for sharing that protected enrollment only with other approved and authorized companies. This is particularly likely if consumers are made aware that any time a company requests authentication against their voice enrollment they have the right to deny the company access to

their original enrollment for authentication by simply choosing not to respond to the request for their voice biometric. As was suggested in the FSTC study, if consumers were to receive appropriate preparation from financial institutions and their industry associations highlighting the advantages of voice authentication and the resulting reduction in identity theft and credit card fraud, it is possible that consumers would support or even encourage their financial services providers to offer voice authentications.

Voice Biometrics For Financial Institutions

Looking initially at credit card issuers, of 290MM+ people in the U.S., approximately 185MM have at least one credit card, and the average cardholder has three bank cards (American Express, Discover, MasterCard, and/or VISA), as there are 700MM in circulation. Approximately 700MM retail and other credit cards are also in circulation, as well as 160MM MasterCard and VISA debit cards.

If you focus initially on the top 10 credit card issuers, they have between 20MM and 100MM cardholders, each totaling around 75 percent of the credit cards issued in the U.S. Consequently, if over the next five years each of the top 10 issuers decided to build closed-voice authentication systems behind their individual firewalls, then the Multiple Enrollment model would take effect and consumers would register for numerous services. Conversely, if just two or three top issuers chose to work together to build a shared voice biometrics registry, a critical mass of 50MM to 100MM consumer enrollments could be attained, creating a neutral registry for enrolling, storing, and managing voice biometrics for the financial services industry and allowing consumers the option for a Single Federated Enrollment.

This is where we find the financial services industry today. Do companies individually enroll their customers behind their firewalls and keep the enrollments for their exclusive use, or do they work with third parties that share the use of the enrollments with a limited number of approved and authorized companies? Following the lead of the FSTC, banking industry organizations such as MasterCard and VISA are researching the federated model and how it could benefit their members and consumers. In addition, newer entrants in the financial services industry, such as PayPal, are researching integration of voice authentication into their core customer service operations. In the case of PayPal, nearly all of their 30MM customers need to occasionally or regularly transfer money to or from their checking or credit card accounts, and better authentication would eliminate significant opportunities for fraud.

With expense justification being the overriding concern of financial institutions today, the decision to implement voice authentication surpasses their initial hurdles, since Return On Investment models demonstrate a potential 3-to-1 or 4-to-1 savings over expenses. For instance, a credit card issuer with 25MM cardholders would enroll the majority of their customers within 24 months during the activation calls required before using a new or renewal card. Simultaneously, they would integrate voice authentication into their customer service call centers in place of touchtone or spoken entry of the cardholder's 16-digit account number and/or 9-digit Social Security number (when calling from their home, office, or mobile phone perhaps) for the 100MM inbound calls they receive per year. The expense reductions from not needing live operators to request your mother's maiden name and from eliminating 30 to 60 percent of account takeover cases when identity thieves call in using a fraudulently obtained account number and Social Security number make the case for adopting voice authentication.

Next, the financial institutions address their initial instinct to build the voice biometric registry behind their firewalls for their exclusive use, since they are covetous of cardholder information and concerned about outsourcing a call authentication function. However, over time they note that they are countering strong industry trends toward outsourcing functions that require heavy investment in early-stage, rapidly changing technologies based on new expertise they do not have in-house. Finally, they appreciate that an exclusive voice biometric database is a large new cost center, but that if they share the enrollments (with their customers' permission) they can participate in the revenues that accrue to a neutral registry from outside organizations authenticating against their cardholders' enrollments – which can turn their cost center into a brand-new profit center.

Voice Biometrics For Direct Merchants

If a Single Federated Enrollment model develops, the second industry that will want to integrate with the voice biometric registry is telephone retailers (again, such as Dell and LL Bean). By authenticating the identities of inbound callers who read a credit card, they can capture a voice biometric and compare it with the enrollment associated with the credit card. Telephone order merchants typically find that fraudulent transactions can amount to as much as 1 to 4 percent of revenues, so a \$1BB revenue base means that cutting transaction fraud in half can be worth \$5MM to \$20MM in savings. An additional feature of capturing a voice file from a caller is that if the transaction later turns out to be fraudulent, the retailer retains a biometric recording of the caller instead of just a fraudulent credit card number and sham shipping address. These recordings could then be used to assist law enforcement agencies with finding and prosecuting identity thieves with far greater success.

After integrating voice biometrics into their telephone transactions, direct merchants could add voice authentication to their online sales, which can have fraud rates even higher than those of telephone transactions. In the near term, at the end of an online transaction the website could prompt you to enter a phone number which would then be dialed for your voice authentication, or an 800 number could be provided for you to call and enter a given code number before making your voice authentication. In addition, companies such as Dell that offer free telephone technical support for their products would be able, for the first time, to easily authenticate callers as true customers before allowing access to the highly paid technical support reps they maintain for troubleshooting.

Voice Biometrics For Healthcare Providers

On April 14, 2003, the first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers took effect. Developed by the Department of Health and Human Services (HHS), these new standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed. Congress directed HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA includes provisions designed to encourage electronic transactions and also requires new safeguards to protect the security and confidentiality of health information.

Under HIPAA, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of protected information needed for a particular purpose. In addition, patients have to approve a specific authorization before a covered

entity can release their medical information to a life insurer, a bank, a marketing firm, or other outside business for purposes not related to their health care. Obtaining specific written advance permission from patients for every conceivable use of their health records may prove extremely cumbersome. A more patient-friendly option is for healthcare providers to use voice authentication in combination with inbound or outbound phone calls to gain voice-authenticated approval to share patient records on an individual basis.

Companies such as Merck are researching voice authentication as a means of providing proof of consumer authorization. While healthcare providers could enroll consumers for later authentications, utilizing an existing neutral registry of enrolled voice biometrics would significantly improve the economics of using voice signatures as confirmed authorization.

Voice Biometrics For Government

While consumer privacy groups have historically been concerned that biometrics registries could lead to big-brother monitoring by government, the increasing support by consumers for security and anti-fraud technologies has created the opportunity for government to offer voice biometrics to constituents in a positive light. Federal agencies that provide information to consumers, such as the Social Security Administration, Internal Revenue Service, Census Bureau, and Medicare, could either choose to enroll consumers directly or authenticate against a Single Federated Enrollment. Another obvious potential is the use of a voice enrollment registry for authenticating travelers boarding airlines, ships, and trains, as well as at international borders, as an alternative to adding a biometric-on-a-chip in passports and comparing those to travelers – the latter requiring that tens of thousands of biometric readers be installed at airports worldwide.

The Voice Biometrics Ecosystem

The registry of 24MM toll-free telephone numbers now managed by NeuStar helped create a multibillion-dollar market for 800-number services in the long distance industry and supported the creation of direct response advertising and the entire direct merchandising industry. The registry of 25MM domain names now managed by VeriSign provided a scalable naming system that, in combination with the browser and mass adoption of Internet access, helped support the creation of e-commerce companies, search companies, and online content providers, and provided a new channel for consumer-focused companies to communicate with their customers.

The development of a neutral registry of voice biometrics for consumer enrollments and authentications could similarly create billions of dollars of efficiencies for consumers and the companies with which they do business. In turn, an entire industry of supporting products and services could develop that would have far larger revenue potential than the registry itself. Initially, a cottage industry would spring up to provide user interfaces and integration between customer call centers and the voice biometric registry, along with the bandwidth providers that would carry the transmissions. In addition, numerous top-tier integrators and consultants would work with Fortune 500 companies to adopt voice authentication into their customer relationship processes, just as happened with Web design and integration.

Longer term, as more consumers become comfortable with the voice registration process and the number of companies integrating voice authentication into their business practices grows, you can imagine the numerous times in a month that you might voice-authenticate calls to financial services providers, insurance providers, healthcare providers, government agencies, retail merchants, etc. While you might initially use voice authentication just a few times a year with your credit card issuer, over time it is possible to foresee authenticating several times a month and eventually several hundred times a year. With each industry that adopts voice authentication, a wide range of companies could generate millions and billions of dollars customizing products, services, and technology solutions to meet the changing needs of consumers and industry.

The Future Of Voice Biometrics (And Why It Could Start A Wave Of Innovation)

When AT&T created the initial 800-number database, or when the U.S. Commerce Department created the first database of commercial domain names, the originators could not possibly have anticipated the long-term effects of their creations. Similarly, when positing the creation of a voice biometric registry it is beyond the imagination to foresee all of the potential uses and adaptations that established companies and entrepreneurs will dream up. But having spent two years looking at potential paths of interest and talking with numerous companies in a range of industries, I believe breakthroughs are not only possible but highly likely in several areas:

Telephone Banking – All of the major credit card issuers have other lines of business, such as checking accounts, insurance, auto loans, and mortgages, which typically have separate call centers and require entry of different account numbers and PINs for authentication. In time, voice authentication will help financial services providers offer a single 800 number for their customers to access and manage any of their products or to transfer between them. Voice authentication makes possible automated servicing of high-value/high-risk transactions such as wiring money, transferring funds, and stock trading, without having to provide thousands of call center employees with access to a customer's registered secrets, such as birth date, Social Security number, or mother's maiden name.

E-Signatures – Companies that require live signatures on transactions are required to send paper confirmations by mail or fax for you to sign and return by mail or fax. Rather than going online to fill out a mortgage, stock transaction, insurance, or other legally binding form and then having to apply pen to paper, a voice biometric can be electronically attached to the online document. All you would have to do is call an 800 number, touchtone in a provided code number, and authorize a specified online document with a voice signature approval.

Remote Card Transactions – Once consumers become used to authenticating telephone transactions by voice it would not be a significant leap in consumer education to equip gas pumps or ATM machines with microphones and Internet connections to the voice biometric registry to confirm transactions. Just think of the ExxonMobil SpeedPass – except instead of a device on your keychain you would use your voice, and instead of it being usable at a limited number of locations, it could work at any terminal where you are required to swipe a card or enter a PIN number.

E-Commerce Transactions – In the short term, retailers might voice-authenticate telephone transactions or even use a telephone call to authenticate online purchases. But, as the number of households with broadband connections grows from the current 18MM to 60MM+, more consumers will utilize

telephones or microphones that are integrated with their home computers. That way, you could go to Amazon, buy something, be prompted over your computer's speakers to voice an authentication into your computer's microphone or telephone, and consequently be assured that identity thieves cannot make purchases on your account. Voice authentication, in such a scenario, could actually provide a compelling application for consumers to integrate their PCs and telephones or to buy PCs with embedded telephone features.

Delivery Services – When you order products to be delivered, the merchant could request a Voice On Demand in order to be sure that you, and only you, receive the product. For a company such as eBay, to be able to eliminate the uncertainty as to whether a buyer or someone else received a shipped product could provide a greatly increased level of security to individuals who sell products to distant buyers.

Telecommunications Services – Think of all the times you enter your PIN number into your voicemail system at home or work or on your wireless phone. With a single voice biometric enrollment you could eliminate hundreds of touchtone authentications a year. In addition, your voice could be used to authenticate and easily set up features such as call forwarding, conference calling, and calling card calls. In addition, if your wireless phone were set up to require a single voice authentication each time it was turned on, your handset would become worthless to thieves.

In each of these areas, biometrics is on the verge of reinventing the authentication process quickly, efficiently, and profitably. New technologies are coming to market just as consumer acceptance for biometrics is reaching a historic turning point. All that is required to make biometrics take off is for a few top companies in a couple of industries to take a leadership role in introducing biometrics to consumers on a mass scale, which will familiarize and acclimate the general public with the process and instill confidence with the systems in place to protect them.

I hope I have stimulated your thinking about biometrics and whether it might become a Hot Technology for 2004 and beyond. At the very least, our vision does not suffer from a lack of grandeur, since the goal is to enroll almost everyone in the U.S. – and someday the world – while integrating the majority of financial service companies and other industries with a neutral shared voice biometric registry. I look forward to your comments in the next issue of SNS, or you may contact me directly through SNS if you have questions that you wish held in confidence.

With an authentic voice, I am,

Bob Nelson
President, Nelson & Company
McLean, Virginia
VP and Board Member, TradeHarbor, Inc.
SNS Member # 189

Copyright ©2003 Bob Nelson, all rights reserved.

About the Author

Since 1987, Bob Nelson has structured alliances between early stage technology ventures and Fortune 500 companies that integrate or remarket new products and services optimized for their customer bases.

Through Nelson & Company, Bob is currently Vice President of Partner Development and on the Board of Directors for TradeHarbor, Inc. (www.tradeharbor.com), a St. Louis-based voice authentication service. Previously, he served as the Entrepreneur in Residence for VeriSign, following a merger with Network Solutions, in their Northern Virginia new business incubator. He also co-founded and was Chairman and CEO of CrossMedia Networks, a pioneer in providing email-by-phone services, and advised speech recognition services provider PriceInteractive, which is now Convergys Speech Solutions.

Prior to Nelson & Company, Bob developed his background in marketing alliances at MCI Third Party Marketing and with Satellite Business Systems. He has also served on the staffs of Retired Chief Justice Warren Burger and United States Senator Pete Wilson of California. He came to Washington, D.C., in 1978 with Congressman Doug Bereuter of Nebraska.

I would like to thank Bob again for taking the time to make these arguments to the SNS community. Those seeking additional technical information on the voice vs. other authentication techniques can find it at the tradeharbor site listed above.

With the announcement that a Pakistani computer user cracked the Microsoft Passport system this week, potentially exposing buckets of personal information, one has to continue to wonder at the wisdom of aggregating large amounts of critical private data into centralized databases. This has been one of the greatest hurdles facing those in the Homeland Security organization seeking critical vulnerabilities in the nation's infrastructure, public and private: no one wants to put them into a central database. I suspect that solving this problem lies at the center of a path that would allow massive authentication to move forward.

That said, it's hard to think of a more useful authentication tool than voice. One can imagine the usual objections: tape recording fakes, what happens if the person is unable to speak, or if the voice has changed drastically for some reason (stress, illness), are the error rates truly competitive, and so on. But, providing there are good answers, voice has got to be near perfect.

Your comments are always welcome.

Sincerely,

Mark R. Anderson

President

Strategic News Service LLC

P.O. Box 1969

Friday Harbor, WA 98250 USA

Tel. 360-378-3431

Fax. 360-378-7041

Email: sns@tapsns.com

INSITES

SNS readers interested in additional predictions and information can turn their browsers to:

The SNS website, at <http://www.stratnews.com>.

SNS Members' Corner, at

http://www.tapsns.com/subscriber_corner.shtml

SNS Members' Gallery Spotlight Page:

<http://www.tapsns.com/spotlight.shtml>

The Orca Relief Citizens' Alliance, a 501(c)(3) non-profit effort to study and reduce Orca mortality rates, supported largely by technology workers. Please visit our new website, at <http://www.orcarelief.org>, for more information. Contributions may be sent to: ORCA, Box 1969, Friday Harbor, Washington, 98250.

The Hybrid Vigor Institute, at <http://hybridvigor.org> focused upon providing tools and environments leading to great new discoveries in interdisciplinary science.

New to the Family:

I would like to welcome, among others, these new members to the SNS Family: Paul Terry, CTO, OctigaBay Systems Corporation, Burnaby, BC; Andrew Waitman, Managing Partner, Celtic House Venture Partners Inc., Kanata, ON; John McGrath, Dell Computers, Inc., Round Rock, TX; James Hong, Founder, HOTorNOT.com, Mountain View, CA; James F. Moore, Senior Fellow, Harvard Law School, Berkman Center for Internet & Society, Cambridge, MA; Andreas Bechtolsheim, Authora Inc., Seattle, WA; Klaus Stapf, Saxony Economic Development Corporation, Dresden, Germany; Laura Dodd, Senior Account Executive, Waggener Edstrom, Bellevue, WA; and many others.

SUBSCRIPTION INFORMATION

If you are not a subscriber, the prior Strategic News Service item has been sent to you for a one-month trial. If you would like a one-year subscription to SNS, the current rate is \$495.00 U.S.,

which includes approximately 48 issues per year, plus special industry alerts and related materials. Premium Subscriptions, which include passworded access to additional materials on our website, are \$795.00 per year. Subscriptions can be purchased, upgraded or renewed at our secure website, at: <http://www.stratnews.com>. Conversion of your trial to full subscription will lead to thirteen months of SNS, no matter when you convert.

VOLUME CORPORATE SUBSCRIPTION RATES: Below half price, upon registration with SNS for a minimum of ten subscriptions at \$1950.00. SMALL COMPANY (10 employees or fewer) SITE LICENSE: \$995. TEACHERS' GROUP RATE: (five teachers): \$195.00.

STUDENT and INDEPENDENT JOURNALIST RATE: \$195.00 per year.

This service is intended for strategic thinkers who depend upon business technology planning. The SNS charter is to provide information about critical computer and telecommunications issues, trends and events not available to managers through the press. Re-purposing of this material is encouraged, with proper attribution. Email sent to SNS may be reprinted, unless you indicate that it is not to be.

If you are aware of others who would like to receive this service, please forward this message to them, with a cc: to Mark Anderson at sns@stratnews.com; they will automatically receive a one-month free pilot subscription.

About the Strategic News Service

SNS is the most accurate predictive letter covering the computer and telecom industries. It is personally read by the top managers at companies such as Intel, Microsoft, Dell, Compaq, Sun, Netscape, and MCI, as well as by leading financial analysts at the world's top investment banks and venture capital funds, including Goldman Sachs, Merrill Lynch, Hummer Winblad, Venrock and Warburg Pincus. It is regularly quoted in top industry publications such as BusinessWeek, Newsweek, Infoworld, Institutional Investor, Wired, the Financial Times, the New York Times, and elsewhere.

About the Publisher

Mark Anderson is president of Technology Alliance Partners, and of the Strategic News Service(tm) LLC. TAP was founded in 1989, and provides trends and marketing alliance assistance to firms leading the convergence of telecom and computing. Mark is a Seybold Fellow. He is the founder of two software companies and of the Washington Software Alliance Investors' Forum, Washington's premier software investment conference; and has participated in the launch of many software startups. A past director of the WSA, Mark chairs the WSA Presidents' Group. He regularly appears on the Wall Street Review/KSDO, CNN, and National Public Radio/KPLU programs. Mark is a member of the Merrill Lynch Technology Advisory Board, and is an advisor and/or investor in Authora, Ontain, Ignition Partners, Mohr Davidow Ventures, and others. He also serves on the board of the not-for-profit Hybrid Vigor Institute, and is a principal in the investment advisory firm Resonance Capital Management LLC, which

manages the accounts of institutions and high-net-worth investors, focused on technology markets.

Disclosure: Mark Anderson is a portfolio manager of a hedge fund. His fund often buys and sells securities that are the subject of his columns, both before and after the columns are published, and the position that his fund takes may change at any time. Under no circumstances does the information in this newsletter represent a recommendation to buy or sell stocks.

On May 19th - 22nd Mark will host the SNS Future In Review Conference, at the Hotel del Coronado, in San Diego. Contact sam@tapsns.com, or go to <http://www.futureinreview.com> for more information. On September 9th, he will offer the opening keynote speech on the current state of wireless communications, at the WSA Tech Future Conference, Westin Hotel, Seattle. And on September 18th, he will provide the keynote speech at the Financial Executives International meeting in Las Vegas.

In between times, he will be listening to good friends and great minds, sharing new ideas about what will happen just outside the easy-time window, and walking one of the most beautiful beaches in the world.

Copyright 2003, Strategic News Service LLC

ISSN 1093-8494