Current Issues in Technology Management

FALL 2004 ISSUE 4, VOLUME 8

SATM

STEVENS ALLIANCE FOR TECHNOLOGY MANAGEMENT

DIRECTOR'S NOTE

This issue is devoted to a provocative article by Dr. Niv Ahituv, in which he foresees a new era for society -- the open information era. The time is approaching, Dr. Ahituv argues, when the cost of protecting information will become so high, and computer networks will proliferate so widely, that individuals and organizations will for the most part give up efforts to protect their private databases, and society will become an open information society.

Dr. Ahituv explains why an open information society is inevitable and how it will be reached. This will clearly have profound implications for individuals, business, and government. Society will necessarily become much more selective about secrecy, and will turn to various "social safeguards" to prevent undesirable consequences. Dr. Ahituv considers the potential concerns and the implications for regulation.

Niv Ahituv is Academic Director for the Center of Internet Studies, Tel Aviv University. During the 2003-2004 academic year, he was a visiting professor in the Howe School of Technology Management at Stevens Institute.

Larry Gastwirt

STEVENS Institute of Technology

The Open Information Society: *A World Free of Secrets*

Dr. Niv Ahituv

Try to imagine life without secrets.

Forget your first reaction (almost certainly something like, "Oh, that's impossible.") Let's assume, for the sake of argument, that it is possible. Sort of like in George Orwell's science fiction classic, "1984". But our example has a very powerful tool that Orwell couldn't even imagine: the computer.

What does that have to do with it? According to a well known principle in Cognitive Psychology, a person is able to pay attention simultaneously to seven chunks of information. So if screens at home monitor everyone, at work and in the streets, then one-eighth of the population is required to monitor the other seven-eighths. However, people need to rest, to eat, to work on shifts; therefore three-eighths should watch the other five-eighths. But what about managers, controllers, service personnel and the like? Apparently, in Orwell's low-tech futuristic fantasy, nearly half the population would have had to be retained to observe the every move of the other half. He never dealt with one critical question: who was going to observe all of the observers? However, Orwell's vision augmented with computers and a communication network is feasible and horrifying.

If we take this notion of life without secrets a step further, into the twenty-first century, it isn't hard to imagine a world that Orwell never even considered.

Continued on next page

The Open Information Society...

Continued from cover

Let's say you're the top compliance official at a midsize West Coast brokerage outfit, and the following report is waiting for you on your desk one morning:

DAILY REPORT

Date: . . . . . .*March 27*

Time Block: . . . . . .*4:00 - 8:00 PM*

Subject: . . . . . .*Joseph K.*

Occupation: . . . . . .*Senior Trader*

Work Place: . . . . . .*Pacific Stock Exchange*

Home: . . . . . .*2424 Truth Avenue, Los Angeles*

Gender: . . . . . .*Male*

Personal Status: . . . . . .*Married*

RECORDED ACTIVITIES:

4:17 PM - Subject left office; source: corporate energy monitoring computer noted the lights in his office extinguished and turned off the air-conditioning.

4:19 PM - Subject left building; source: corporate clocking-in system.

4:24 PM - Subject left parking lot; source: electronic gate computer scanned the license plate of his car.

4:35 PM - Subject bought gasoline at Shell station, 11733 Knowledge Blvd. (Reference: opposite direction from his home); source: credit card company computer.

4:51 PM - Subject parked at Beverly Hilton Hotel, Beverly Hills; source: National Traffic and Parking Center computer.

4:58 PM - Subject charged bottle of champagne and sushi platter to his credit card. The refreshments were delivered to Room 434; source: credit card company computer. Crosscheck: Room 434 was registered to Maria S.; source: hotel guest registrar records. Maria S. is CFO of Bradley International Freight (BIF), one of the leading freight forwarders on Pacific Basin routes.

6:12 PM - Subject phoned two numbers in Osaka, speaking for less than one minute in each conversation; source: Telephone company computer.

6:21 PM - Subject left hotel parking lot; source: National Traffic and Parking Center computer.

7:12 PM - Subject returned home; source: house maintenance computer.

OTHER RELEVANT DATA:

A. In trading on the Tokyo Exchange today, BIF shares are up 12%; source: Tokyo Stock Exchange computer.

B. Joseph K. has told his secretary he will arrive late today, but asked her to watch for interesting developments in the freight forwarding industry; source: verbal communication.

C. Maria S. flew to Tokyo 87 minutes after checking out of her room at the Hilton; sources: hotel computer, immigration authority computer, airline company computer.

RECOMMENDATION:

Summon subject for further investigation. Freeze his personal trading accounts. Notify the SEC ASAP. Suspicion: Insider trading. Secondary Suspicion: adultery.

Each of the computerized monitoring functions detailed here exists today. All that's missing to make reports like this one reality is the networking function that could link them all. Moreover, after the tragic events on September 11, 2001, special software was installed in most of the Internet service providers, software that enables the interception of messages transmitted through the net, based on the detection of keywords, suspected e-mail addresses, and some more advanced algorithms of Artificial Intelligence.

The proliferation of cellular phones is going to increase the level of personal exposure by an order of magnitude. Right now the location of each cellular phone customer can be identified whenever the customer carries the phone. However, very soon the cell-phone will become the major means of payment, replacing the credit card. The customer, upon reaching the supermarket cash register, for example, will dial a certain code and a payment authorization will be transmitted to the supermarket computer. Similarly, our cellular phones will handle payments at vending machines, in gas stations, drug stores and the like. Consequently, the monthly statement of the cell-phone company will become a detailed logbook of our whereabouts through the entire month.

It all begins in your mailbox. More specifically, with all those letters and catalogs that used to be called junk mail but have lately been elevated to the august category of direct mail. They are not only in our regular post but they also flood our electronic mailbox today under the titles of SPAM, personalized banners, pop up ads and the like.

Sometimes, you have to wonder how all these people know you exist. It's obvious, of course -- they buy your name along with thousands of others from companies whose products you've ordered -- but it's amazing nonetheless to see how fast your name can leapfrog to the marketing department of every company. Add to that the use of new software tools named *Data Mining* and you'll understand why after purchasing toddler toys you are more likely to receive an ad for pampers and not an ad for a new health program for elderly people.

When you phone in your orders to these companies, you're often surprised to find that the operator needs only your name or an identifying code; the company's computer already knows the rest of your particulars: address, ZIP code, telephone number, credit card number, sometimes more.

How did all of that information get there? When you understand that, you understand the essence of the Open Information Society. You might not have noticed, but in the past few years, the world has found out a lot of things that you might think are none of anybody's business. Actually, every business or administrative transaction that you perform vis-à-vis a company or a governmental agency, either in writing or through the telephone, not to mention via the Internet, generates a digital trail that can be followed by others, integrated with other digital footsteps that you have left, analyzed and stored forever.

...every business or administrative transaction that you perform vis-à-vis a company or a governmental agency, either in writing or through the telephone, not to mention via the Internet, generates a digital trail that can be followed by others, integrated with other digital footsteps that you have left, analyzed and stored forever.

Do you really think you have a private life? Let's look at who knows all kinds of things about you. The Department of Motor Vehicles, the Internal Revenue Service, the Social Security Administration, the Franchise Tax Board, either the Republican or Democratic national party, VISA, MasterCard, American Express, TRW, every bank you've ever dealt with, your travel agent, any airline whose frequent flyer program you've ever joined, your telephone company, the electric company, all sorts of professional organizations, local government, board of education, utilities and more.

Each of them knows anything you've ever told them, as well as all sorts of other sundry information someone may have passed on to them. When a travel agency that promotes trips to Spain buys a list of all American Airlines frequent flyers that visited Iberia in the past two years and your name is on it, the agency knows you're a good prospect, and you'll appear that way in its database until someone decides otherwise.

Just as we have little or no control over who gets into our mailboxes and how, large and small companies are equally helpless when they try to control who gets into their computer systems and what they do there. Most try to build electronic barriers around databases and online information, but people who want to get in tend to be quicker.

For years, hackers, crackers, industrial espionage agents and spies have been

Continued on page 4

The Open Information Society...

Continued from page 3

cracking codes and passwords, and breaking into the computer systems of companies, governments and military agencies. Since the end of the Cold War and the fall of the Iron Curtain, spying has focused increasingly on sophisticated electronic espionage aimed primarily at obtaining industrial and economic information.

As soon as any company, organization or public body senses a breach in computer security, they rush to pad the layers of protection that guard secret information. But the attackers are determined, and they have the upper hand. Regardless of how many millions or billions of dollars are spent on computer security, the infiltrators always seem to get what they're after.

How long can this go on? As long as companies and public agencies refuse to let go of the notion that secrecy is of the utmost importance, and as long as the public refuses to give up on some of the privacy that has been elevated to a God-given right in some Western countries.

In other words: not much longer. Society wastes billions of dollars each year trying to keep curious people out of information that doesn't belong to them. But the barriers just pique the interest of hackers and saboteurs of all kinds. Eventually -- soon -- advocates of computer security will relent. Their motivation will be largely economic; not only is protection too expensive, but database owners who open up their databases will be able to tap into a lucrative source of cash-flow: access fees charged to outside users.

The main barrier to the Open Information Society (OIS) is psychological -- and it can be overcome. The sooner you stop saying it will never happen, the sooner you'll set your sights on getting ready for the biggest revolution since Thomas Edison discovered electricity.

The solution is simple: remove most of the barriers, open the information to anybody who wants it, charge access fees for use... and watch the world transition into an Open Information Society.

The main barrier to the Open Information Society is psychological -- and it can be overcome..... (get ready for) the biggest revolution since Thomas Edison discovered electricity.

For skeptical readers, let me remind you that not very long ago, software products were protected against illegal copying by various means: passwords, laser burn, hardware mechanisms, limited number of copy availability, and more. All those techniques that prevailed in the mid-1980s failed. Why? Because it was "payable" to copy a piece of software whose price was $500 and up and save those high prices. But once the prices of office products became "reasonable", customers were willing to buy a legal copy and the support that follows rather than an illegal copy. Since the 1990s we aren't seeing attempts to protect regular software products. Still, it seems that the software companies make profits. I believe that a similar phenomenon will develop in the information market.

This isn't an Orwellian fantasy. It's a sober analysis of reality, circa 2000s. Just look at a few of the signposts on the road to the OIS:

- If your loan application is turned down today, all you need to do is call TRW, the giant collector of credit history, to find out what blemishes on your record made your bank deem you a bad risk. If you have any reason to doubt your credit worthiness, you can check with TRW in advance to get a good idea of what to expect from lenders.
- For a few thousand dollars one can subscribe to a computerized database of military information that includes explicit details about some of the latest American military developments.
- Students all over the world are taking classes via "virtual education," which enables enrollment to expand to hundreds of thousands of students, each of whom is able to study independently with the aid of PCs and modems. Many schools already let students "attend" videotaped lectures at their convenience via the Internet.
- More and more people who clock in and out of work no longer use time cards at all; they simply run a magnetic card (or a

smart card) through a little machine at the front door. The information gets recorded on a central computer and from there it's easily accessible to all sorts of authorized or unauthorized users. Not outside your company, perhaps, but surely within it. As the OIS approaches, the scope of access will broaden. Why not forward these data to the IRS for example?

- Most commercial banks have developed information systems that offer customers more services than were thought possible a few years ago. One-stop stations at the branch and Internet services at home let you do just about all of your banking transactions at one terminal. Increasing numbers of customers never talk to tellers anymore.

- The Internet serves as a commercial channel that connects businesses to customers (B2C; e.g., Amazon), businesses to businesses (B2B; supplier to their customers, for example), customers to customers (C2C; e.g., e-Bay), governments to citizens (G2C), and the like. Consequently, being connected to the Internet becomes a matter of survival to many organizations. However, if you are connected you are also exposed to raids on your data.

- Many providers offer data communications and Internet access services to anyone who wants to subscribe. It's much more than subscribing to a telephone company. Users can access a large variety of public databases containing commercial, industrial, and scientific information (such as Dow Jones, Official Airline Guide, Defense Department procurement proposals, articles in chemistry, physics and engineering, and much more). And, like the world of telephone service, consumers have seemingly endless options.

- Systems-integrating computers and satellite communications are proliferating. Some nationwide truck companies, as well as some military forces, install inertial location systems (ILS) in each vehicle. Through satellite communications, the location of a car or truck can be pinpointed within a few yards. The ILS helps companies locate each truck in their fleets, or trace stolen cars. In military applications, an ILS can provide the central command with exact details of its force deployment. It's even being used to fight auto theft. For a few hundred dollars, you can have a transmitter hidden in your car. If it gets stolen, all you do is report your membership number and the company locates your vehicle in seconds. However, by using the same system, a maintenance service company can locate the exact whereabouts of its technicians, a parcel delivery company can trace the exact route taken by its employees, and the chief of police can tell exactly where his or her subordinates are spending their time.

- Other applications of similar technology can be found in prison parole programs. Rather than hold people in jail or force parolees to visit their parole officers every few days, so-called electronic handcuffs are used with increasing frequency. They aren't really handcuffs at all. Rather, the individual wears a bracelet equipped with a tiny transmitter that emits signals that are monitored by the police or other authorities. If the person strays beyond preset boundaries, his keepers will know about it and take appropriate action.

- The introduction of digital electronic switchboards into telephone networks has opened up the possibility of identifying callers before you answer the phone (Caller ID). The identifications of the callers are also accumulated in the telephone company databases, where the information can be analyzed for commercial purposes.

- In most retail businesses the cash register reads the magnetic strip on the back of the credit card and electronically transmits details of the transaction to the credit card company. As debit cards catch on, the same principle is applied, except that the cash register sends an order to the bank to debit the user's account immediately. The purchase profile of each card holder is now available to the credit card company where it can be used for data mining and forwarding to other retail companies.

Continued on page 6

The Open Information Society...

Continued from page 5

All of these developments are the result of the mind-boggling computer revolution that has unfolded in the past two decades. These rapid leaps in computer technology are the prime catalysts in the move toward an open information society. But there's more; the rapid developments of electronic media and communications tools, as well as the profound growth in human awareness and literacy of information technology, have expanded potential access to information bases.

The examples cited in this article paint a picture that points in a clear direction. Without ever voting or making a formal decision, the world has opted for the Open Information Society.

A few years ago, they were the domains of a small elite; today anyone can access them.

It all comes down to the old adage: If you can't beat 'em, join 'em. Like hackers and copycats, busybodies are a fact of life, and nothing that anybody can do will make them disappear or back off. Society has two choices: either it can keep up the exasperating and expensive -- especially expensive -- game of cat-and-mouse, always striving to stay half a step ahead of the legions who want access to secret information; or it can decide to be more selective about secrecy. This second option may mean changing some conventional wisdom, and that will take time, but once the transition is complete, all of those billions that have been wasted on security will be freed for constructive use.

The examples cited in this article paint a picture that points in a clear direction. Without ever voting or making a formal decision, the world has opted for the OIS. Just look at all the things you can access today that were beyond your reach a decade ago. The trend is clear.

What can be done? Accept that technological progress is uncontrollable. What, then, are the means we can employ to prevent undesired developments? Apparently, we are left with social safeguards such as education, laws, regulations, treaties, voluntary and statutory organizations, and the like. We could call them controllable parameters. They are essentially creations of social agreements motivated by social concerns about potential dangers and threats.

There are several main issues crying out for legislation, regulation, and international treaties.

These include the following:

INFORMATION MONOPOLIES:

The threat of information monopolies makes the antitrust field very important in the OIS. What will happen when two companies in the same industry have access to the same databases? Are they allowed to share information, for free or even for charge? What if they decide to merge?

DATA ACCESS EQUITY:

Open information should be equally open to every potential user. This implies that owners of databases (see next) should tell the public how to access each database and how to retrieve information from it.

But the threat always remains that if a database is too friendly, too many people will be too free to access parts of it not intended for them. In addressing this question, lawmakers will need to consider how such openness can coexist with whatever right to privacy remains. Equality should be maintained also for those who do not have the means to possess information technology of their own.

INFORMATION ACCURACY:

Database owners must protect data from falsification attempts. The term "open information" relates mainly to the freedom of retrieval. When it comes to changing and updating databases, there should still be protection which must be regulated by law. However, who is responsible for the accuracy of the data when the owner and the source are not the same entity?

BREAKING INTO AND THEFT OF DATA:

Thought must be given to a new definition of "stealing" and "breaking and entering." The so-popular act of computer hacking and cracking is not well defined yet. When is an outside user guilty of stealing information, and when is he or she merely accessing something that is open to all? Is breaking into an Internet site without changing existing data, but rather leaving a trace or adding data, illegal? The hacker did not take anything but only left something.

INDIVIDUAL RIGHTS:

Three key liberties must be preserved and guaranteed by law: the right to know, the right to appeal and the right to NOT make a few specific types of information accessible to others. For obvious reasons, these rights need not apply to databases that essentially provide catalog access to previously published material. If, for instance, you maintain a newspaper

clipping database, you should not be required to inform people each time their name appears in the database. Similarly, a library does not have to report to the authors of the books that their names appear in the catalogue.

COMMERCE LAW:
No one has yet taken a very profound, careful and comprehensive look at commerce laws, but they surely need revamping. Without speedy recognition of the fact that the OIS means new laws are needed, the entire information revolution could be derailed.

INTELLECTUAL PROPERTY:
A few years ago, enemy number one of the music, film, book and software industries was the physical copying of their products on DVDs, CDs, and video cassettes, known by the term piracy. Common to all those products is that they are informational products, hence piracy is easier, faster and cheaper than, for instance, copying the design of furniture or the taste of a good wine. The problem has been amplified by an order of magnitude in the Internet era. Now the pirate does not have to physically ship the copied product but can rather forward it through the network.

CYBERCRIME AND CYBERTERROR:
The advent of the Internet has created a new category of crimes: Cybercrime. This term refers to various types of crimes performed over the Internet: sending viruses and worms, forwarding SPAM mail, distribution of illegal material such as child pornography, and performing all sorts of sting operations via e-mail, from convincing innocent people to send money to rescue someone in distress to seducing young girls to come to a blind date with someone who pretends to be of a different identity or personality. Cyberterror can be performed by hacking and cracking into the computers of government agencies, utilities, defense agencies, airlines and many others and trying to create all sorts of chaotic disorder. Simple flooding of a certain Internet site with millions of messages can paralyze a public service or business for a significant time.

All of these issues will need to be dealt with effectively in the coming Open Information Society. ■

About the Author:

Niv Ahituv is the Marko and Lucie Chaoul Chair for Research in Information Evaluation and the Academic Director for the Center of Internet Studies of Tel Aviv University. Past positions he has held at the University are Vice President and Director General (CEO), Academic Director of the Center for Global Business, and Dean of the Faculty of Management of the Graduate School of Business Administration. During the 2003-2004 academic year he was visiting professor at the Howe School of Technology Management.

From 1996 to 1999 he was Chairman of the Board of Maalot, the Israeli securities rating company (an affiliate of Standard and Poor's). He was a member of the Intergovernmental Information Technology Committee of UNESCO and represents the Government of Israel in all information-related issues discussed in UNESCO. Dr. Ahituv is co-author of *Principles of Information Systems for Management*, a widely used textbook

SATM

STEVENS ALLIANCE FOR TECHNOLOGY MANAGEMENT

UPCOMING EVENTS

SEMINAR

Assessing and Improving the Alignment of Information Technology with the Enterprise

November 3

The third of a Seminar Series in Technology Management, sponsored by SATM in collaboration with the Columbia University School of Engineering, will take place on Wednesday, November 3rd, 6:30 - 9:00 PM at Columbia. The speaker is Dr. Jerry Luftman, Executive Director of Graduate Information Systems Programs and Distinguished Professor of Information Systems at the Howe School of Technology Management.

Business-Information Technology (IT) alignment refers to the application of IT in an appropriate and timely way, in harmony with business strategies and goals. The importance of effective alignment between the IT function and the business is well accepted. Less well understood is how to assess the degree or maturity of alignment, and how to improve it. Firms often find it difficult to harness the power of IT for their long term benefits, even though there is much evidence that IT has the power to transform whole industries and markets.

In this seminar, Dr. Luftman will describe his framework for evaluating business-IT alignment, and will present the results of some of his research on enablers and inhibitors for achieving mature alignment and leveraging the impact of IT on the firm.

Combined Roundtable and SATM Advisory Board Meeting

November 15

The next SATM Roundtable meeting will be held on Monday, November 15 from 1:00 - 5:00 PM at Stevens. It will feature three presentations by Howe School faculty members on their research. The faculty presentations will be preceded by a brief Advisory Board meeting. All attendees are encouraged to attend the entire combined meeting and to partake in a buffet luncheon from 12:00-1:00 PM.

For further information on these and other Alliance activities, contact Dr. Lawrence Gastwirt: **212-794-3637 • lgastwirt@aol.com**

INFORMATION

Visit the SATM website: **http://howe.stevens.edu/SATM**

To download articles from past SATM newsletters, go to **http://howe.stevens.edu/SATM/Newsletters**

To send comments on this newsletter, or to submit an article for future publication, please e-mail Dr. Jack McGourty at **jm723@columbia.edu**

SATM- Stevens Alliance for Technology Management
Wesley J. Howe School of Technology Management
Stevens Institute of Technology
1 Castle Point on Hudson, Hoboken, New Jersey 07030

Sharen Glennon 201-216-5381 sglennon@stevens.edu

STEVENS Institute of Technology