



INC PLAN (USA)

26-C Trolley Square
Wilmington, DE 19806
Tel: 800.462.4633
302.428.1200
Fax: 302.428.1274
www.incplan.net

If you are serious about your business...incorporate

SPECIAL REPORT

Issue: Personal and Financial Privacy

Jacques Luben



Moderator
LiveInvestorsForum.com
26-C Trolley Square
Wilmington, DE 19806
Tel: 302.428.1200
Fax: 302.428.1274
jluben@liveinvestorsforum.com

Please contact LiveInvestorsForum.com for more information.

Our two expert panelists can be reached directly as follows:

Mark Nestmann



Editor
Sovereign Society
Newsletter
Tel: 888.358.8125
www.sovereignsociety.com

Caroline Quigley



Executive Vice President
Inc Plan (USA)
26-C Trolley Square
Wilmington, DE 19806
Tel: 800.462-4633
www.incplan.net

Participants:

Mark Nestmann - Editor of the Sovereign Society newsletter. He has written a number of books (including How to Achieve Personal and Financial Privacy in a Public Age). He is also a prolific author of special reports that instruct investors about their rights. Most recently, Mr. Nestmann has been instructing North Americans about how to "globalize" their personal and financial affairs in order to minimize the ongoing encroachment of Big Government and Big Business.

Caroline Quigley - Executive Vice President of IncPlan (USA), a Delaware based incorporating firm that helps investors set up companies that provide corporate anonymity on the Web. Ms. Quigley is also the editor of the firm's newsletter.

Jacques Luben - Moderator of the Webcast, Executive Director of LiveInvestorsForum.com, is a widely quoted investment expert who developed precious metals programs at Morgan Stanley Dean Witter and Merrill Lynch. He recently completed his tenure as President of Platinum Guild International, a mining trade association.

Are Personal and Financial Privacy Still Possible in an Age of Big Government, Big Business and Intrusive Technology?

Main Topics:

1. How to identify the multiple privacy risks that are related to the explosive growth of the Internet?
2. Where are the best offshore locations to invest from a privacy viewpoint?
3. How can a Delaware corporation provide complete individual privacy as you "surf" the Net?
4. What is the best way for private individuals to avoid frivolous lawsuits?
5. How to avoid electronic and paper "junk" mail

“...about as secure as a post card sent through the mail.”

Mr. Luben began by asking Mr. Nestmann what he considered the worst privacy threat facing computer users today? Mr. Nestmann responded that people who use e-mail and post information on news groups put themselves at risk when they don't realize that they are using an insecure medium. Adding to the risk, their information is permanently archived and available for retrieval for years.

Identity Theft

Turning to the issue of identity theft, Mr. Nestmann described how each year, about 500,000 people have their identity stolen:

“Identity theft occurs when a thief uses your Social Security Number, or in Canada your Social Insurance Number, to find out enough other information about you to build a usable profile of the victim. This kind of information is readily available over the Internet or from information brokers. It's very inexpensive.”

While the Social Security Number is the single most important piece of data for a thief, now, simply knowing someone's birthday, address or telephone number can lead to identity theft.

Mr. Nestmann told the story of a female lawyer in California.

“Someone stole a few pieces of her mail, which included a credit card application. The thief then applied in the woman's name but used her own address. She was able to go onto the Internet and find her victim's social security number and then apply using that social security number but a different address and then had the credit card mailed to the address of the thief.”

While credit card companies are becoming more vigilant, their methods are by no means fool proof and the discrepancy between the two addresses went unnoticed. The thief ran up \$50 to 60,000 of bills, ruining the victim's credit rating before she was caught.

The Internet is a rich area for thieves because “there is so much information and it's protected so poorly.” He pointed to online banking services, easy to access with just a social security number, and to motor vehicle and telephone records which are rich in data as examples.

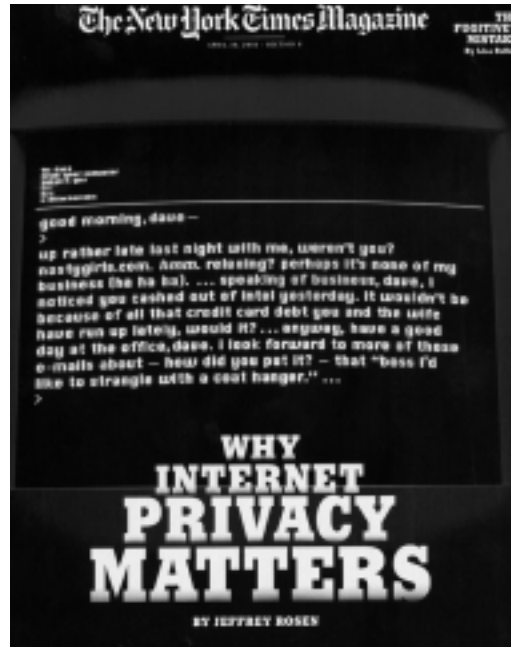
Mr. Nestmann described the hacking of CD Universe. 30,000 credit card numbers were stolen from this web site. The hackers demanded payment from CD Universe. When ransom was not forthcoming, the hackers posted the credit card numbers online, freely available to the criminal world.

'Cookies'

Mr. Luben asked about the mechanisms which allow commercial web owners to gather information about visitors to their sites; commonly known as 'cookies.' Cookies, according to Mr. Nestmann are:

“little bits of text that a web site can send to a location on your hard drive. So they're stored on your computer, not at the web site. And what happens is that the next time you visit the web site the web site computer will ask your computer if it has a cookie. And if it has a cookie it will indicate that you've visited that web site and perhaps even what pages you've visited. Where it gets threatening is when you match that with information in direct marketing data bases. For instance, a internet company called Double Click recently purchased a company called Abacus Direct. Double Click is the biggest publisher of banner ads on the Internet

and they're a big user of cookies. Abacus Direct on the other hand is one of the largest direct mail and direct marketing companies in the world. When you merge these two data bases, not only will you have a record of the source of catalogue purchases and so on from the Abacus Direct data base, you will also have a record of where they've been on the web, courtesy of the Double Click data base. So the combination of these two data bases has a lot of people quite concerned because the potential for privacy invasion and profiling of consumers is now even greater.”



Unfortunately, Mr. Nestmann believes that the government is part of the problem rather than the solution. Because the government's technology for research and protection is two or three years out of date, it is imperative that consumers take immediate self-protective action.

In his book *"Practical Privacy Strategies For Windows 95/98,"* Mr. Nestmann details solutions and preventative efforts. These range from tools to turn off the cookie in a browser to techniques like anonymizers, remailers, encryption or steganography which allow the preservation of anonymity on the Internet, in e-mail and in news group postings. These "off the shelf" software packages do not require advanced computer skills to install and use.

Mr. Nestmann feels strongly that not only should individuals not wait for government protection but the government itself is a stealth collector of information. He cited the National Security Agency, known as the NSA, which has over 250 listening posts globally. These monitor Internet, telephone and fax communications for content, key words, voices of people they want to identify, etc. Mr. Nestmann advocates "A little bit of safeguarding right now of your PC can go a long way to preserving your privacy."

Hiding Your Identity

Turning to Caroline Quigley, Mr. Luben asked her to describe her company, Inc. Plan (USA,) and the method of masking an individual's identity by surfing the web as an anonymous corporation. She stated:

"In some states, the laws that govern corporations actually allow a certain amount of anonymity. In Delaware, for example, they allow a great deal of anonymity. So at Inc. Plan we developed the idea that the corporation could become your privacy proxy on the Internet. By using that anonymous corporation, you could, first of all, open accounts in the name of the corporation, you could have a credit card in the name of the corporation. Instead of having a Social Security Number you could use the corporation's tax payer id number. Your anonymous Delaware corporation should be your vehicle for surfing the Internet, for sending e-mail. Besides providing you with anonymity it could also contain damage should anything catastrophic happen. With a corporation, you will not be responsible for any fraudulent activity and it would end right there, it would not spill over into your private life and your personal credit rating would not be affected."



Mr. Nestmann agreed with Ms. Quigley's ideas and suggested the further precaution of installing and registering Windows 95 or 98, and the computer itself, in a corporate name.

Moving Money Offshore

Mr. Luben asked the best ways to move and keep money offshore legally. Mr. Nestmann responded that the safest way is probably wire transfer and that there are intermediary companies that will, for a fee, move money. He added that there are no tax advantages in placing money in an offshore corporation, unless it is actually conducting active business offshore with management, or at least the preponderance of that management, being offshore.

Mr. Nestmann noted offshore banks are unlikely to disclose information because in their home countries, for instance Switzerland, the Bahamas, the Cayman Islands, Austria, Luxembourg and Liechtenstein, information release without a court order is a criminal offence.

Everbank, found at www.Everbank.com, as one of the few online banks to have solid, up-to-date security.

E-Mail Questions from LiveInvestorsForum.com Visitors

- “Can the average person install software to keep your internet privacy or do you need a special technician?”

Mr. Nestmann replied that it is not only possible but easy to install the precautions oneself. His book *“Practical Privacy Strategies For Windows 95/98”* shows installation procedures step by step.

- “Are Delaware corporations better or worse than Nevada corporations?”

Ms. Quigley stated “for privacy, there’s no question that Delaware is much, much better” because the state does not require filing names of corporate principals. She added that whether you incorporate in Delaware or Nevada, you are “insulating your private assets from the corporate assets. So in that respect a corporation in either state will give you protection. But true privacy is only available in Delaware.”

Civil Forfeiture

Mr. Luben asked about civil forfeiture, the process “whereby the government can seize your property without convicting you of any crime then force you to prove you are innocent in order to get it back.” Mr. Nestmann responded that legislation had passed in the House last year to reform the civil forfeiture process, but was now bogged down in the Senate. Meanwhile, these seizures are bringing in billions of dollars a year that do not go to the general fund. The money goes to the law enforcement agencies, which have every incentive to maximize seizures.

When the civil forfeiture program was instituted in 1984, it was to fight the war on drugs. Now, however, it has reached the point where “it’s perfectly OK for the government to go in and seize someone’s property without convicting them of any crime and forcing them, at their own expense, to prove that it is their property and that they are innocent in order to get it back.” The legal theory, held up in part by the Supreme Court, is that the asset, the moment that it was earned or used illegally, vests to the government. After the seizure, a person has ten days in most jurisdictions to

file a claim to retrieve the asset. After that, one must hire an attorney, post bond, which is usually ten percent of the seized property, and then file a notice with the court of the intention to fight the seizure in court. If these procedures are not followed, there is a five year period for the government to finalize the forfeiture, claim the property as its own, and then sell it for profit.

Privacy Protection Measures

According to Mr. Nestmann, the following are the easiest and most effective ways to protect oneself from potential privacy problems from the Internet:

1. Follow the precautions outlined in *Practical Privacy Strategies For Windows 95/98*.
2. Turn off ‘cookies’ in your browser
3. Log on to the Internet with a computer and an operating system registered in a corporate name.
4. Use anonymizers when visiting a suspect web site. By logging on to an anonymizer service, the service acts as an intermediary. This ensures no hostile program can insinuate into your computer and damage your hard drive or spy on the computer and send information back to the web site.
5. Employ Ms. Quigley’s idea of the Delaware corporation as a privacy proxy.
6. For additional protection from the government, Mr. Nestmann suggests an offshore bank account. His company, The Sovereign Society has relationships with three banks that he strongly recommends.

Contact Mr. Nestmann and the Sovereign Society at www.sovereignsociety.com. In the United States, the representative office can be reached at 888-358-8125. Outside the United States, the headquarters in Ireland can be reached at 353-51-844068. The Sovereign Individual. “is a person who has been able to order his life in such a way so as to reduce his dependence on government for providing the types of services that he needs in order to go about his daily life, whether it be banking, whether it be in the realm of the Internet, whatever it is.”

Ms. Quigley and Inc. Plan can be reached at 800-462-4633 or their web site at www.incplan.net.