

Brought to you by <http://www.KeepYourAssets.net>



**Disclaimer:** We do not give legal or tax advice. The following information is offered only as a point of view. You are encouraged to evaluate this information and act according to your own reasoning and conclusions. Because we encourage independent thought and personal responsibility, we do not accept credit or liability for the use or misuse of this information.

## **TRADITIONAL PRIVACY JOINS THE DIGITAL REVOLUTION**

by Duncan Frissell

### **I. Introduction**

In 1948, when George Orwell needed a title for his dystopian novel about Big Brother and the Ministry of Truth, he reversed the number 48 and entitled it Nineteen Eighty-Four. You remember Nineteen Eighty-Four: an all powerful government using advanced technology to establish an unbreakable tyranny over the minds, souls, and bodies of humanity. In the event, Mr. Orwell was wrong. It hasn't quite worked out that way. Tyrants are looking a little worse for wear these days. What went wrong? In a word \* telecommunications. You'll hear a lot of talk today about the dangers and possibilities inherent in these new toys that we play with. But I want to put things in perspective and talk about some traditional privacy techniques and how they can assist us all in preserving our privacy against government-led assaults on our liberties.

Even after a century of remarkable changes, we are stuck with the tendency to imagine that the world of the future will be like Today only "More So." The Computer and Network transformation of human society that we are exploring today is revolutionary. It will bring many changes that are impossible for us to imagine. The reason things are a little hard to predict is that the main effect of all of the changes we are seeing is to give more and more power and more and more choices to individuals.

If you doubt this, consider this fact: William Jefferson Blythe Clinton is not vastly more powerful than was Louis XIV. Both of these men could destroy a city such that no stone was left standing upon stone. However, the "peasants" of today's rich countries are much more powerful than the chained serfs of 18th Century France. The average American or Brit of today can take two week's salary and buy a computer more powerful than all of the electronic computers that existed on earth in 1955. Or he can take that same money and jet anywhere on earth at almost the speed of sound.

These new powers, multiplied by all the choices that can now be made by billions of individuals, are causing control problems for the world's governments and prediction problems for all of us.

One way of trying to get a handle on this future is to talk about the techniques that have traditionally been employed by individuals to secure their private choices \* their privacy, their independence. This can offer us guidance as to what may happen when everyone comes to recognize that they are free.

One hears a lot of complaints about invasions of privacy these days. But most of the complainers are looking to others to guard their privacy. If you are really worried about your privacy, there are plenty of things you can do to secure it for yourself.

Whatever your personal views about privacy, it is important that you know what is possible now and in the future. Because you can be assured that as the technologies we are talking about today become available, more and more people will use them.

As I talk about some traditional privacy techniques, I want you to keep in mind the sort of future in which these methods will be used.

## **II. The Fibersphere**

In a forthcoming book, the American commentator George Gilder calls this future the Fibersphere \* the networked world in which communications is so cheap as to be almost free. A world in which anyone who wants to can communicate privately with anyone else and one in which no outsider can read, never mind block, that communication. It will be a very different world indeed. How will people use some of the capabilities that other speakers here today have discussed? Let's see what they've done in the past.

## **III. Privacy Techniques**

In the seven decades since the growth of the modern interventionist state, people have been developing and deploying many techniques to preserve their privacy. These powerful planning techniques have offered many individuals and companies the opportunity to arbitrage the effects of personal and financial regulation by the nation state.

### **A. Concealment as a Privacy Technique**

The basic privacy technique is that of concealment \* not telling others that information which you wish to safeguard.

#### **1. Keeping Secrets**

Much of what we are talking about here today deals with our fears of a loss of privacy, with our concern that the new technologies will destroy this recently won privacy.

Our ability to keep secrets has come and gone through the years. What we think of as privacy is a fairly recent phenomenon. There was very little privacy in the 14th century in an English castle crammed with retainers (or in an English village in the 20th century for

that matter). Privacy grew with bourgeois society and with the city. Getting lost in the crowd and living in small family households increased our concept of privacy.

## **2. Private Communications**

It used to be that we were at least able to communicate privately with those we met in person. And, of course we could only conduct private conversations in person.

We could also more or less trust the privacy of the contents of our letters posted in sealed envelopes.

With the telegraph and telephone and radio came the ability to speak with people thousands of miles away. But it created the opportunity for others to listen in with wiretaps and electronic bugs.

Computer networks now allow inexpensive long distance communication. But they have proved to be rather insecure. However, the spread of military- grade encryption enabled by powerful computers will bring back private communications. In addition, the sheer volume of communications will make it very hard for unintended eavesdroppers to filter out the specific messages they are trying to intercept. Here's an example of the sort of thing we can expect:

## **3. Telephone Forwarding**

It's December 1st, in the year 2000 and President-elect Clinton calls me for advice on how to deal with the tax compliance problems her administration will face. The White House switchboard places a call to my communications server (think of it as a distributed process -- a software robot) running on several computers "somewhere on the nets." This is, of course, a digital phone call and travels to my communication server as a series of groups of zeros and ones, called packets.

My communications server (a combination answering machine, electronic mailbox, and receptionist) handles all of my indirect contacts with the rest of the world. Hillary's call passes the criteria I have programmed into my server and so is forwarded to my location somewhere on earth. The path that the packets that make up this call take is convoluted and passes through a number of commercial remailers. These remailers mix the packets with other genuine and phony voice and data communication streams, then readdress them, and eventually forward them to me (but with such speed that neither Hillary nor I notice the lag). If done properly, these remailers will allow me to have a real- time conversation with the President-Elect of the US without her being able to trace the call, even if she were to employ the entire resources of the US government.

The phone call I've just described is an example of how networks can enhance what I call locational ambiguity.

## **B. Locational Ambiguity as a Privacy Technique**

About 25 years ago, a friend of mine faced a problem. He had received a "job offer" from the United States government. They had invited him to visit scenic Vietnam and interact

with the native cultures. In fact, they insisted on it. When John, a New Yorker, received his notice to report for a draft physical exam, he immediately moved to California. He then wrote his New York draft board saying that he was in California and had no funds to travel to New York for his physical. After a few months, his records were transferred to a California draft board, and he received another notice to report for a draft physical. He immediately moved to Texas and repeated the process. He finally got a letter from the Texas draft board which not only ordered him to report for induction but also ordered him to stay in Texas. He immediately moved to Tennessee and sent a letter of regret to the Texas draft board apologizing for having already left Texas.

Repeat until end of war.

Disguising your actual location is convenient for a number of reasons beyond avoiding conscription. Aside from being a shield against government intrusion, locational ambiguity lets you take advantage of the varying legal regimes. It confirms one major advantage that we all have over the Nation State — we can move and the State (absent war and an invading army) can not.

Note the effect of disguising your true residency -- governments treat residents very differently from non-residents. Residents are taxed, regulated, counted, and tracked. They are called for Jury Duty, sometimes prohibited from owning gold or foreign currencies, or conscripted. On the other hand, visitors are treated much more leniently. In America, foreigners can do all sorts of things that citizens cannot and are free from many of the burdens. The message is clear. If you want to be well-treated, be a guest rather than a resident. Residential ambiguity helps you keep your exact status fuzzy. And there are several ways of achieving this ambiguity.

### **1. Accommodation Addresses**

The most frequent personal question any of us is asked is, "What is your name, address, and phone number. Many of the dossiers that are built up about us are based on our address.

Traditionally, one would secure one's privacy and keep one's physical location uncertain by using an accommodation address. These so-called private mail boxes or mail receiving services, have proliferated in recent years in America.

Using accommodation addresses, one can not only protect oneself from problems like, say, cyborg killers tracking you down, as Arnold Schwarzeneger did to the poor woman in *The Terminator*. But this method also can handle more mundane annoyances such as those from salesmen or from the Inland Revenue.

Small businesses can use a mail receiving service to show a prestigious address that differs from their actual address, or perhaps to establish a presence in another state or another country.

By changing your address, without having to move, or keeping your exact address uncertain through the use of mail receiving services, you can reduce the harm to your privacy involved in the misuse of your actual address.

## **2. Telephone Answering Services and Voice Mail as another form of ambiguity.**

In most cities in the US today, I can pick up the phone, call a computer- based voice mail service and get a unique phone number and account in 5 minutes. The disadvantage of a traditional answering service is that everyone can tell it is an answering service. Voice mail avoids this problem. This voice mail account sounds just like a normal telephone answering machine. I record my greeting and can change it any time I like. I can dial in and retrieve my messages. This is a real world example using today's technology of the sort of future communications server I described above.

## **3. Future Locational Ambiguity**

In a very short time, it will be very hard to tell exactly who you are dealing with, where people are, or what they are doing. Networks care little about such questions. From this room, I can easily and cheaply connect to and use computers in Japan or Australia and do work or import data. By shattering time and distance, networks weaken the geographical bonds that governments depend upon to exert their controls.

While governments are weakened by computers and networks, private bureaucracies also find themselves increasingly transformed.

## **C. Multiplication of Entities as a Privacy Technique**

The formation of independent business entities is a privacy planning technique as old as that one great contribution of Mercantilism -- the corporation. The ability to have an independent entity (an artificial person) under your control but legally separate from you has always been very convenient for enhancing privacy.

During the 1920s, Alfred Carl Fuller became one of America's first black millionaires because his thousands of door-to-door salesmen and millions of customers never knew that the Fuller Brush Company was owned by a black man.

### **1. Business Explosion**

As capitalism progressed, the number of types of business forms has exploded. Partnerships, trusts, corporations, limited partnerships, limited liability corporations are common in today's business world.

### **2. Declining Corporate Size**

As the number of business enterprises has grown in recent years, in the US and Europe, average company size has plummeted as computers make it easier to shop around for the goods and services that you need for a business project. If I can hire a 747 or a hundred temporary packaging engineers with a few phone calls, I have less need to keep a large staff on site. And if the sort of work you need done can be done over the nets, the people you hire or contract with can live anywhere in the world.

### **3. Everyone an Entrepreneur**

The future of computers and networks will make things even looser. It will be possible to throw together virtual corporations on a project basis to get something done. One can also create and manage many different sorts of entities with ease.

One can already buy shelf companies in a few minutes using credit cards over the telephone. Imagine what sorts of instant entities can be created in a networked world. It will be possible to use smart computer software to create synthetic business entities as easily as securities dealers have created synthetic securities. Those who work for these temporary entities will be able to meet together using future virtual reality interfaces, even though they may be thousands of miles apart.

### **4. The Securitization of Life**

I call this multiplication entities the "securitization of life." First there were stocks and bonds. Then there were futures contracts and options. Now there are options on futures contracts, futures contracts on options, and derivatives too complex to describe.

Computers and networks make it so easy to create new forms of business relationships and ownership that the ability of regulators to regulate them will be severely compromised. A good example of this problem is the whole area of financial services.

### **D. Foreign Banking and Financial Services as a Privacy Technique**

Everyone here is familiar with the stories of "foreign bank accounts." Financial services are what we are really talking about when we discuss tax havens and the traditional financial privacy community. People have been moving some of their financial affairs to other countries for years. They have, traditionally, had many reasons to do so.

#### **1. Reduced Political Risk**

Many of those who choose to bank in jurisdictions in which they do not live do so to reduce their risks of losing their money to their government or to lawsuits. They have considered it important to avoid putting all their eggs in one basket. It is always safer to keep some of your wealth in countries in which you do not live.

#### **2. Enhanced Services**

Others have chosen to deposit funds in other countries' banks to secure services not available at home. It is still very difficult for Russians to have a bank account, so they have been frantically opening accounts in Western banks. If you live in the US and want an account denominated in a foreign currency, the only practical way to do so is to open a foreign bank account.

#### **3. Choice of Tax Jurisdiction**

Obviously, the holders of foreign accounts have also sought friendlier tax jurisdictions. Whether legally or illegally, they have placed their funds in tax haven bank accounts where no local tax liability accrues and where they may be able to minimize their tax liabilities back home.

#### **4. Network Banking**

When I talk about the future markets on the networks, people always say things like, "What can you sell over a fiber optic cable?" This failure of imagination can be avoided if we look at some of the things that are already being bought and sold over the nets. Financial services are the easiest to be transformed by the new computer and telecommunications technology and the single easiest "digital service" to sell over the nets.

In fact, this is already happening. The international traders in securities, foreign currencies, and derivatives have developed a transnational computer linked market for their "goods." Take the forex market. It has tripled in size since 1986 reaching a daily volume of one trillion dollars. The reason for the collapse of the EECs Exchange Rate Mechanism is the simple fact that the world's governments who together possess about one trillion dollars in foreign exchange reserves are helpless to control an international market whose daily volume alone equals their entire level of reserves.

In the past, only wealthy individuals and companies could take advantage of the tax planning and other financial benefits of offshore banking. Within a few years, sophisticated international financial services using strong encryption technology and the sort of anonymous forwarding I've spoken of before will be as close as everyone's networked home computer. This will render financial regulation a real challenge for governments. This will happen because the real power of networks lies in the fact that they make "action at a distance" easy.

#### **E. Expatriation as a Privacy Technique**

When one feels hassled in a particular community, a natural response is to move away. When you are moving away from a nation, it is called expatriation.

When we think of traditional expatriates, we think of someone like Marc Rich who fled the US in the late 1970s to avoid federal prosecution. With his new Spanish Citizenship and hundreds of millions of dollars, he currently resides in Switzerland. The Feds had accused him of profiting from Jimmy Carter's price controls during the Oil Shock of the 1970s. He bought "old oil" which was subject to price controls and magically transformed it into "new oil" which was not. Interestingly enough, since he left the US, his firm Clarendon Ltd. continues to sell copper and nickel to the US Treasury to mint coins.

The new expatriates who will be coming along in the next few years will be able to employ ever more sophisticated technology to accomplish some remarkable feats.

#### **1. Permanent Traveler (PT)**

An ancient privacy-enhancing technique is to become a permanent traveler or PT. From the gypsies of Europe's past to temporary residents of the South of France today, PTs have always gained partial exemption from the geographically based controls imposed by the nation state. In recent years, a fair number of people have intentionally become PTs.

Note for example, that the US taxes the income earned by its citizens or permanent residents no matter where on earth that income is earned. Even that quite strict regime, however, does not claim to tax the earnings of Brits or Germans dodging the gunfire to visit Walt Disney World in Orlando, Florida.

In the same way, if I, a US passport holder, am traveling in France and Germany while setting up a leveraged buy-out in the US using my cellphone and my laptop, I am not violating the laws of those countries concerning work by foreigners without a work permit. And I have no effective French or German tax liability for the profits derived from these activities.

The significance of these facts today is that it will soon be possible to manage a Fortune 500 corporation, direct a "film", perhaps even perform surgery while traveling hither and yon about the world. That will make it rather difficult for the revenue authorities of the OECD countries.

What happens when some future version of Madonna notices that she can eliminate tax liability by expatriating herself while still selling her services over the nets?

## **2. Virtual Expatriation**

Now not everyone feels like moving overseas. The disadvantage of traditional expatriation is that you had to leave home and move to a strange land where people may not even speak your language. In addition, you have to leave all of your social and business contacts behind. Also, it usually meant that only wealthy individuals with very portable jobs could take advantage of expatriation. Modern networks improve this situation by making possible virtual expatriation over the nets, even if they're working at home.

The South of France or Thorshavn in the Faroe Islands or Peoria, Illinois are right next door to each other on a network. With appropriate encryption techniques, large numbers of people will be able to work from anywhere to anywhere. This will mean in practice that they can remain physically in a high-tax country while they conduct their business "offshore" with lower effective tax liabilities. Everyone who cares to be will, in some sense, be international.

## **F. Internationalization as a Privacy Technique**

The international realm has unique legal characteristics. While I can't advertise unregistered securities or foreign bank accounts within the US, I can advertise them in international publications. The regulations which govern specific actions taken in international transactions are very ambiguous.

The thing about current and future computer networks is that they constitute an international publication. To a network, nationals are foreigners, foreigners are nationals and everyone is international. For example, someone outside the US can use the Internet to import controlled cryptographic technology from the US, in spite of the fact that it's a violation of US law for anyone in the US to export that technology. Non Americans can

take advantage of the First Amendment to the US Constitution to read and publish materials over the nets that might be illegal in their home country.

Living in an international world means in some sense living outside of the realm of the nation state. Absent the imposition of a world government (which would seem to run counter to the direction the world is currently heading) things are bound to get quite a bit looser over the next few years.

#### **IV. Conclusion**

This loosening is a matter of concern for many people. Both law enforcement personnel and the general public worry that the new technology will be used for pornography, for organized criminal activity, or for terrorism. This is not a problem unique to computers and telecommunications, however. Many different sorts of modern technology have increased the capabilities of individuals to do good or evil. The advantage of the network revolution is that -- unlike other technologies -- it offers the tools to solve the problems it creates. On the networks we can filter out unwanted communications. We can build digital webs of trust so that we can live and work only with people who recognize the rights of others. Traditional methods of social control will not work well over the nets. We will have to develop new forms of social interaction that emphasize individual responsibility and self control.

And what can we call this new form of social organization growing on the nets and in the modern fluid business environment? When two or more people can meet together and communicate freely and privately without interference by outsiders, they can trade -- they can form a market. If this trade on the nets is made free from even the possibility of external regulation, what we have is a free market and a free society.

Delivered at the First European Conference on Computers, Freedom and Privacy.  
London. November 1993.