4

Rivendell

part 1

THEORY & PHILOSOPHY OF PRIVACY

By way of introduction to our Seminar, we each offer our views on, (1) the need for privacy, and (2) the prospects of achieving it. Later, we will provide more detailed lectures on specific privacy topics. After each such presentation, you will have an opportunity to ask questions, contribute ideas, argue with us or whatever. The venue will be a moderated list. Thank you for signing up for Privacy 101. We hope you will find it provocative, enlightening and rewarding.

Sandy Sandfort
Duncan Frissell
September 1994

332 Bleecker St., #F-34
New York, NY 10014
USA

PRIVACY: WHO NEEDS IT?

by Sandy Sandfort

Curiously, I've never had much interest in privacy, per se. In part, this is because extreme, personal openness is an almost uniquely American cultural trait. For me, it's a personal one as well . It is one, however, from which I have been weaned by sometimes bitter personal experience and the "horror stories" of others.

THE BAD NEWS

What I'm concerned about is freedom. Unfortunately, there are those who are offended by the freedom of others, and seek to rectify the "problem". And information about you is one of the most effective weapons they have. Protecting your privacy keeps that weapon out of their hands. Whether you seek privacy for its own sake or to keep vital information out of the hands of enemies, your privacy is imperative. The "intelligence" in the names of the CIA, DIA and various law enforcement agency departments refers to the gathering of secret information for military or police purposes. Non-governmental organizations and individuals seek and use intelligence, too. Without the ability to gather intelligence, none of them can have much power over you. With good intelligence, it's another story. It can tell them your habits, your routine, your strengths, your weaknesses, where you sleep at night... where your family sleeps at night. There are wolves in the woods whether we choose to admit it or not. Unless you are absolutely sure you have--nor ever will have--any enemies, prudence dictates a low profile .

It is clear that information about you in the wrong hands, puts you at risk. By the same token, it is NOT clear that information about you in anyone's hands does you much good. Promiscuous dissemination of personal information makes you vulnerable to every sort of societal predator. To address such risks, you need to organize your life in such a way that your personal information can be made available only on a limited and conditional need-to-know basis. In addition, proactive steps can be taken to enhance, alter, duplicate, substitute or camouflage such information. (More on this later in the Seminar.)

What information should you protect? "Everything" is a good first approximation. For years, the amount of peanut butter used at military bases has been classified. The reason? It's trivial to determine manpower deployment if you have base-by-base figures for peanut butter consumption. A similar correlation has been made between late-night pizza orders from the Pentagon and the initiation of hostilities in such places at Granada, Panama and the Arabian Gulf. Obviously, though, some types of information are more critical than others. We will be discussing specific areas of concern in upcoming lectures. But what is far more important than merely enumerating specific threats, is getting yourself in the habit of "thinking privacy." If you are like me, "thinking privacy" does not come naturally, it must be learned. Hopefully, by the end of this Seminar, you will be automatically identifying and avoiding privacy pitfalls in your everyday life.

THE GOOD NEWS

There are those who profess to believe that a decade after the symbolic "1984," it is impossible to keep your affairs private. They are wrong, but such negativism acts as an insidious self-fulfilling prophecy that keeps them from trying. Even worse, their negativism often dissuades others from trying as well. How do I know privacy is possible? Well, for obvious reasons, identifying privacy "role models" is difficult. (Would the picture of the 1994 "Privacy Poster Boy" be just a blank 3'x4' piece of card stock? How about a picture of the Cayman Islands with a human silhouette superimposed on it?) Nevertheless, I have read about, communicated with, met and assisted many such "Privacy Poster Boys." I won't tell you most of their names, but I will verify their existence and share their secrets. The funny thing is, it's not that big a deal. Piece of cake, really. This is a seminar for optimists. Not because of the power of "positive thinking," but because the power of the individual is growing. Because there are many more of us (good guys) than them (bad guys). And because there are millions of folks in the world who are already successfully using the techniques we will be discussing. While there is no reward without risk, the pioneers have already blazed the trail. Please remember that specific threats and their solutions will come later. At this point we only want to shake the nay sayers out of the trees. If you either doubt the threat or doubt that anything can be done about it, PLEASE state your case on the list. We want to address your real concerns rather than just guess what they may be. You may also start asking specific privacy questions at this time. We probably won't address them at this time, but we will have something to say about them later in the Seminar when we cover related subjects. All questions will be treated as confidential. In our public discussions, we will paraphrase, edit and generalize your questions to render them as anonymous as possible. We recommend you encrypt and mail forward questions containing sensitive personal information. We do not need to know your identity. My public key is*

WHY PRIVACY?

That's the easy one to answer. People who are trying to invade your privacy, always ask , "If you haven't done anything wrong, what do you have to hide?" The answer -- "If I knew what I had to hide, I certainly would. Since I don't, I need my privacy." No one can predict what personal characteristics or behaviors will be punished in years to come. When I was born in the 1950's, smoking was a virtue and sodomy a vice. At some time and in some place during the last 200 years in Europe, virtually every human characteristic has led someone to kill someone else. Race, sex, creed, political philosophy, social or economic class -- all these factors have been used to attack people at certain times in certain places. Since some innocent fact about you may at some time put you at risk, and since no one can predict what that critical fact will be, a general habit of privacy preservation pays real dividends. Another answer to the question "why privacy?" is "why not". What right do others have to demand information from you? It costs you time and worry to surrender the intimate details of your life to strangers. If you can get what you want *and* preserve your privacy, you might as well do so. Let the busy bodies that want to know all about your life find something else to do. Put the personal details of your life on a "need to know" basis. You'll save time and worry and frustrate those who are trying to get you to give them free information about you.

PRIVACY YESTERDAY - PRIVACY TOMORROW

Even though you may feel that your privacy is under attack as never before, it's simply not true. A few years ago, humorist P. J. O'Rourke moved to a small town in New Hampshire. After he had been living there for about 6 months, he had occasion to go into a local store to buy some underwear. As he was paying for his purchase, the sales clerk observed, "That's not your usual brand of underwear." The fact is that throughout most of human history, we've lived in tiny communities in which everyone knew everything worth knowing about everyone else. If the authorities

wanted any information about any one, they had merely to ask. Today's world allows many more opportunities to protect your privacy. Even though it may seem that all of us are wrapped in a web of computer databanks, much of that information is unlinked to us and hence unable to harm us. As we shall see in this seminar, there are many additional steps that you can take to protect yourself from modern attempts to rebuild the social control mechanisms of the ancient village. We will also have an opportunity to talk about how some of the traditional privacy techniques - residential ambiguity, multiplication of entities, offshore financial services, etc. can be combined with the latest in net tech to frustrate the attempts of control freaks to "make me dance as they desire with jail, and gallows, and hellfire."

HOUSEKEEPING

This is a moderated list. Most of the major posts will be essays by Sandy and me. We will be editing some of the posts we receive to frame questions that we can answer but if you have general privacy comments, there are other newsgroups and mailing lists which are a better forum for same. We can also be contacted personally if you have individual questions. If you don't know how to use the Majordomo software, send the message -- help -- to majordomo@c2.org

THREAT LEVEL MANAGEMENT--THE CALCULUS OF RISK

When I (Sandy) was in private practice, I had some independent truckers for clients. Before then, I had thought of legality in black-and-white terms. Something is either legal or illegal. Like being pregnant, there's no middle ground--you are or you aren't. But then I learned about the trucking industry. Theory met reality, and theory lost. I went on a couple of runs with one of my clients (I'll call him"Lance"). Just about everything Lance did violated some ICC rule or state law. He ran "hot loads" (cargoes he was not permitted to haul, such as processed foods or manufactured goods), he broke speed limits, his truck loads were too heavy, he went over-hours, carried a gun and took "road aspirin". But it wasn't just he, it was *everybody*. If even only half the truckers in America were to operate in complete legal compliance, we'd all starve and freeze to death in the dark. What Lance *was* very careful to do was comply with the ICC and state rules concerning running lights. If one of his lights burned out, he promptly replaced it. At the same time, he didn't even try to comply with the driving hours rules. The reason? Smokey (Highway Patrolman) can see your lights from his car. He has to stop you to look at your driver's logbook. Because the likelihood of getting caught for a lights violation was much greater than for weight, hours, load, etc., it was "more illegal" in Lance's way of thinking. I called it "variable illegality", but the insight was Lance's. Without formal education, Lance intuitively understood a concept that some MBAs have trouble mastering--cost/benefit analysis. And it's a concept that applies to privacy, freedom and your life, every bit as much as it does to long-haul trucking or business planning. Cost/benefit analysis comes into play in at least a couple of areas of personal privacy. Sometimes taking steps to protect your privacy are inconvenient; sometimes they are illegal. We will freely discuss the "convenience costs" of legal steps we will advocate in this seminar. For obvious reasons, we will not advise you to take any actions that will violate the law. We will, however, try to fairly assess the various "legal risk costs" that some people have accepted to protect their privacy. To illustrate, let's analyze a simple example. When you get a phone line, if you do nothing, your name will be listed in the telephone directory. There are ways this can be avoided, but for the sake of this example, let's just say the only way is to pay a monthly "no listing" fee. Your inconvenience cost is three-fold. First, you have to take the effort to tell the phone company you want to be unlisted. Second, you have to pay a monthly ransom to be unlisted (under $1 in California, I think). Third, you run the risk of missing some opportunities by not being easy to find. On the other side of the ledger, you benefit by making it more difficult for enemies, scam artists, harassers, survey takers and aluminum siding salesmen to get a hold of you. What should you do? Well that depends on the subjective weight you give to each of these

costs and benefits. In my experience,being unlisted has been for more beneficial than costly. Your mileage may vary. The point is, you should make your decision based on at least a cursory analysis of costs and benefits. By doing nothing, you are letting someone else make that decision for *their* benefit. The chances are very slim that their interests will coincide with your interests. As obvious as this may seem, it is counter-intuitive to many participants in the on-going privacy debate. The opposing position goes something like this: "I don't to get in trouble. If I break (or bend) the rules, and I'm caught, I might get in trouble. Therefore, unless you can guarantee that your privacy techniques are 100% safe, I won't use them". The problem with this stance, of course, is that it does not factor in the risk of *not* breaking the rules. The most telling example this century, is Nazi Germany. The "undesirables" who broke the rules and got their money and themselves out, lived. Most of those who followed the rules, died. Cost/benefit analysis only helps if *all* costs and benefits are factored in. If you are looking for an effortless, cost-free, "zero risk" way to protect your privacy, you can tune out now; this seminar is not for you. There is no benefit without cost. However, our experience has convinced us that strong privacy benefits are possible at *acceptable* costs. Below, Duncan has run some of the numbers that prove it. The risk that people most worry about is the risk of legal punishment -- a criminal conviction and jail time. The traditional method of analyzing the risk (per crime) of arrest and conviction is to take the total number of actual prison days "earned" by convictions in some period of time as punishment for a particular crime and to divide that number by the number of those sorts of crimes committed in the jurisdiction during that same period of time. That gives us a "number of days served per crime" number that neatly wraps up the risk of getting caught, the risk of conviction, and the average time served per conviction. Thus if there are (conservatively) 10,000,000 annual acts of tax evasion by US citizens/residents and 400 people are annually sentenced to two years for those crimes, the math looks like this: 10,000,000 crimes 800 person/years (292,000 person/days) "awarded" in total. 42 minutes of prison time served per act of tax evasion. The odds of serving time are thus .00004 or 4 in 100,000. The odds of being murdered in the US average 8 to 10 in 100,000. These risks are the average risks of course. Planning can further reduce them. Our next lecture will examine specific risks associated with identity privacy (or the lack of it).

IDENTITY INFORMATION RISKS

"What's your name?" The most common question used to invade your privacy. "Who are you?" Another version. "Papieren, bitte!" -- from the World War II movies. It seems everyone wants to know who you are. Why? They want to judge you. To determine your guilt or innocence your worthiness or unworthiness for some purpose based on your past activities as documented in their memories or databases. Those of us in the US are in the middle of a long-running debate about whether or not the government should impose a national ID card of some kind. Australia recently defeated one (for now) as did Holland. The French police have started a system of street ID checks in an attempt to find illegal aliens. They are converting what is nominally a voluntary ID system into a mandatory one. Identity-based information systems whether as simple/complex as the county sheriff's brain of the last century or as complex/simple as the data-mined, supercomputed, profiled datasets of this; hold enormous risks for individuals. Let's see what these are.

1) That others will find out who you are. The primary risk. As we move through life, we accumulate alot of "baggage." From our prenatal medical records through the probate of our estates there is a lot of juicy information attached to us. In addition to physical records, there are the personal views of us formed by everyone we meet. We may not mind some of this in formation being shared with some other people, but most of us would like to exercise *some* control over it. The one thing that links all of this personal information together is, of course, the person. You are the "key field" that connects all of this disparate data. I am not speaking only about formal documentation of our activities but also your reputation in the community and general information about yourself. Much of this information when stored

in a networked database is available to thousands of people spread out over uncounted future years.

2) That others will find out what you are. A big part of your identity extends beyond your "name, rank, and serial number" to include your racial or ethnic heritage, religion, political beliefs, hobbies, and other interests. All of these aspects of your identity can cause you problems in certain times and in certain places. It doesn't matter what characteristics you possess. You name one, and I'll give you and example of when and where persons with that characteristic were punished.It doesn't matter who you are. You've got something to hide.

3) That others will find out what you used to be. You have to be aware that when you protect your identity you are not just guarding against the release of *current* information about you. You don't just have to worry about your place in the *current* social environment. You are also making a bet that that environment will not *change* for the rest of your life. This seems a pretty sure loser of a bet. "Are you now or have you ever been a smoker/gun owner/lothario/carnivore?" As I like to point out, when I was born, smoking was a virtue and sodomy a vice. (Note for those incapable of reading English -- the above sentence implies *absolutely* nothing about my view of either smoking or sodomy so no nasty email please). Your social/legal surroundings are sure to change whether you do or not. Are you willing to bet your *life* that some fact about you or activity you engage in will not render you unpopular in forty years? You certainly are making that bet.

4) That others will find out who your children/grandchildren are. Remember -- you are not protecting yourself alone when you preserve the privacy of your identity. Even though the US Constitution prohibits "punishments that work a corruption of the blood" (punishments that extend to descendants) vendettas of various kinds are not unknown. Most of the world's people live in countries where there are laws or strong traditions that "visit the sins of the fathers upon the sons." This works in both directions, of course. If your identity is linked to that of your parents and grandparents, you may find yourself "punished" for their sins.

5) That others will mistake you for someone else. In addition to worrying about your own information trail, you have to worry about being mistaken for other people. Digitally-stored information is usually not based on any personal knowledge. Just like last year's sci.crypt postings, digital information about you just sits somewhere. It may be searched for juicy tidbits but it is rarely verified or modified. Any errors are very hard to correct. You'd better hope that no one makes any mistakes.This problem will grow in future years as the authorities deploy "profiles" as a method of identifying miscreants. Since a profile system is guaranteed to produce plenty of "false negatives," a fair chunk of the future population may be forced to prove their innocence from time to time after they fit some future IRS/Inland Revenue tax cheat profile.

THE RISKS

And what are some of the problems that can occur when peoplelink together disparate information about you? You know the possibilities:

1) Death

2) Imprisonment

4) Loss of property

5) Loss of standing or reputation in the community

6) Loss of professional licenses and permissions

7) Loss of income

In future lectures, we'll teach you how you can integrate identity privacy into your daily life without having to vastly alter your habits. One hint from Barry Reid, author of "The Paper Trap": Give the government the paper it wants, and it will give you the paper you want.

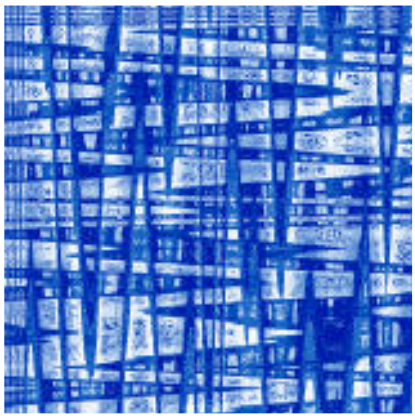
**Email the author for her Public Key via the Majordomo server.*

A Private Citizen.

Rivendell®©


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6

mQCNAi5f89wAAAEEAOiU42TYXhzZGB9GyVUPiphK/V549aDA1KDGccxmPY70ynVt
EUi0Q/X/sHNj73fKCiv6jeoIlagAiamgQT6cL5FGGGkPApyWqrffEClBX67G+mQK
Py+gpGCbDw7FEQPoY4Pfqi0Uf0KMPMBDg1k/djjStVQePNLimYBwiB5FzDvpAAUR
tBtpcmRpYWxAaXJkaWFsc3lzLndpbi11ay5uZXSJAJUDBRAvF7csgHCIHkXMO+kB
AXUhA/9/KthPVRLH6IpgagPK7lZ5qWYM2lhBSxMv9LDKV7nZVRxnsnO55fpQj1r1
popw6JkYAG0BdRTOwUjPhcItyIbEjFGWkmXxDqAjpoKKcpmrajPB6mGtsrZG948A
FxPlPlXqmcg9bGB7x0RYlwZ6baka778MNB8LK15GoUriwUYUPQ==
=FP+2
-----END PGP PUBLIC KEY BLOCK-----
```

Published by pi34 December 1994
irdial@irdialsys.win-uk.net
f. 44+171+351+4858

Issue 4
Thanks to all contributors.
Designed by R-art A.M.D .

Misinterpretations made by the reader/s\
are the responsibility of the reader. Do
not email RIVENDELL with your bullshit.*
Issues 1,2,3 £20 each. Email for details
7482-5192-472-5472-1415-82154-4525-24134
518-381-1816-1541-5235-6556-1515-2862-63