3 April 1997
Source: http://www.infowar.com/class_1/BELL1.html-ssi

Assassination Politics

by Jim Bell

Part 1

I've been following the concepts of digital cash and encryption since I read the article in the August 1992 issue of *Scientific American* on"encrypted signatures." While I've only followed the Digitaliberty area for a few weeks, I can already see a number of points that do (and should!) strongly concern the average savvy individual:

1. How can we translate the freedom afforded by the Internet to ordinary life?

2. How can we keep the government from banning encryption, digital cash, and other systems that will improve our freedom?

A few months ago, I had a truly and quite literally "revolutionary" idea, and I jokingly called it "Assassination Politics": I speculated on the question of whether an organization could be set up to legally announce that it would be awarding a cash prize to somebody who correctly "predicted" the death of one of a list of violators of rights, usually either government employees, officeholders, or appointees. It could ask for anonymous contributions from the public, and individuals would be able send those contributions using digital cash.

I also speculated that using modern methods of public-key encryption and anonymous "digital cash," it would be possible to make such awards in such a way so that nobody knows who is getting awarded the money, only that the award is being given. Even the organization itself would have no information that could help the authorities find the person responsible for the prediction, let alone the one who caused the death.

It was not my intention to provide such a "tough nut to crack" by arguing the general case, claiming that a person who hires a hit man is not guilty of murder under libertarian principles. Obviously, the problem with the general case is that the victim may be totally innocent under libertarian principles, which would make the killing a crime, leading to the question of whether the person offering the money was himself guilty.

On the contrary; my speculation assumed that the "victim" is a government employee, presumably one who is not merely taking a paycheck of stolen tax dollars, but also is guilty of extra violations of rights beyond this. (Government agents responsible for the Ruby Ridge incident and Waco come to mind.) In receiving such money and in his various acts, he violates the "Non-aggression Principle" (NAP) and thus, presumably, any acts against him are not the initiation of force under libertarian principles.

The organization set up to manage such a system could, presumably, make up a list of people who had seriously violated the NAP, but who would not see justice in our courts due to the fact that their actions were done at the behest of the government. Associated with each name would be a dollar figure, the total amount of money the organization has received as a contribution, which is the amount they would give for correctly "predicting" the person's death, presumably naming the exact date. "Guessers" would formulate their "guess" into a file, encrypt it with the organization's public key, then transmit it to the organization, possibly using methods as untraceable as putting a floppy disk in an envelope and tossing it into a mailbox, but more likely either a cascade of encrypted anonymous remailers, or possibly public-access Internet locations, such as terminals at a local library, etc.

In order to prevent such a system from becoming simply a random unpaid lottery, in which people can randomly guess a name and date (hoping that lightning would strike, as it occasionally does), it would be necessary to deter such random guessing by requiring the "guessers" to include with their "guess" encrypted and untraceable "digital cash," in an amount sufficiently high to make random guessing impractical.

For example, if the target was, say, 50 years old and had a life expectancy of 30 years, or about 10,000 days, the amount of money required to register a guess must be at least 1/10,000th of the amount of the award. In practice, the amount required should be far higher, perhaps as much as 1/1000 of the amount, since you can assume that anybody making a guess would feel sufficiently confident of that guess to risk 1/1000th of his potential reward.

The digital cash would be placed inside the outer "encryption envelope," and could be decrypted using the organization's public key. The prediction itself (including name and date) would be itself in another encryption envelope inside the first one, but it would be encrypted using a key that is only known to the predictor himself. In this way, the organization could decrypt the outer envelope and find the digital cash, but they would have no idea what is being predicted in the innermost envelope, either the name or the date.

If, later, the "prediction" came true, the predictor would presumably send yet another encrypted "envelope" to the organization, containing the decryption key for the previous "prediction" envelope, plus a public key (despite its name, to be used only once!) to be used for encryption of digital cash used as payment for the award. The organization would apply the decryption key to the prediction envelope, discover that it works, then notice that the prediction included was fulfilled on the date stated. The predictor would be, therefore, entitled to the award. Nevertheless, even then nobody would actually know WHO he is!

It doesn't even know if the predictor had anything to do with the outcome of the prediction. If it received these files in the mail, in physical envelopes which had no return address, it would have burned the envelopes before it studied their contents. The result is that even the active cooperation of the organization could not possibly help anyone, including the police, to locate the predictor.

Also included within this "prediction-fulfilled" encryption envelope would be unsigned (not-yet-valid) "digital cash," which would then be blindly signed by the organization's bank and subsequently encrypted using the public key included. (The public key could also be publicized, to allow members of the public to securely send their comments and, possibly, further grateful remuneration to the predictor, securely.) The resulting encrypted file could be published openly on the Internet, and it could then be decrypted by only one entity: The person who had made that original, accurate prediction. The result is that the recipient would be absolutely untraceable.

The digital cash is then processed by the recipient by "unbinding" it, a principle which is explained in far greater detail by the article in the August 1992 issue of Scientific American. The resulting digital cash is absolutely untraceable to its source.

This overall system achieves a number of goals. First, it totally hides the identity of the predictor to the organization, which makes it unnecessary for any potential predictor to "trust" them to not reveal his name or location. Second, it allows the predictor to make his prediction without revealing the actual contents of that prediction until later, when he chooses to, assuring him that his "target" cannot possibly get early warning of his intent (and "failed" predictions need never be revealed). In fact, he needs never reveal his prediction unless he wants the award. Third, it allows the predictor to anonymously grant his award to anyone else he chooses, since he may give this digital cash to anyone without fear that it will be traced.

For the organization, this system also provides a number of advantages .By hiding the identity of the predictor from even it, the organization cannot be forced to reveal it, in either civil or criminal court. This should also shield the organization from liability, since it will not know the contents of any "prediction" until after it comes true. (Even so, the organization would be deliberately kept "poor" so that it would be judgment-proof.) Since presumably most of the laws the organization might be accused of violating would require that the violator have specific or prior knowledge, keeping itself ignorant of as many facts as possible, for as long as possible, would presumably make it very difficult to prosecute.

Part 2

"At the Village Pizza shop, as they were sitting down to consume a pepperoni, Dorothy asked Jim, 'So what other inventions are you working on?" Jim replied, 'I've got a new idea, but it's really evolutionary. Literally REVOLUTIONARY.' 'Okay, Jim, which government are you planning to overthrow?,' she asked, playing along.

'All of them,' answered Jim."

Political Implications

Imagine for a moment that as ordinary citizens were watching the evening news, they see an act by a government employee or officeholder that they feel violates their rights, abuses the public's trust, or misuses the powers that they feel should be limited. A person whose actions are so abusive or improper that the citizenry shouldn't have to tolerate it.

What if they could go to their computers, type in the miscreant's name, and select a dollar amount: The amount they, themselves, would be willing to pay to anyone who "predicts" that officeholder's death. That donation would be sent, encrypted and anonymously, to a central registry organization, and be totaled, with the total amount available within seconds to any interested individual. If only 0.1% of the population, or one person in a thousand, was willing to pay $1 to see some government slimeball dead, that would be, in effect, a $250,000 bounty on his head.

Further, imagine that anyone considering collecting that bounty could do so with the mathematical certainty that he could not be identified, and could collect the reward without meeting, or even talking to, anybody who could later identify him. Perfect anonymity, perfect secrecy, and perfect security. And that, combined with the ease and security with which these contributions could be collected, would make being an abusive government employee an extremely risky proposition. Chances are good that nobody above the level of county commissioner would even risk staying in office.

Just how would this change politics in America? It would take far less time to answer, "What would remain the same?" No longer would we be electing people who will turn around and tax us to death, regulate us to death, or for that matter sent hired thugs to kill us when we oppose their wishes.

No military?

One of the attractive potential implications of such a system would be that we might not even need a military to protect the country. Any threatening or abusive foreign leader would be subject to the same contribution/assassination/reward system, and it would operate just as effectively over borders as it does domestically.

This country has learned, in numerous examples subsequent to many wars, that once the political disputes between leaders has ceased, we (ordinary citizens) are able to get along pretty well with the citizens of other countries. Classic examples are post-WWII Germany, Japan, and Italy, and post-Soviet Russia, the Eastern bloc, Albania, and many others.

Contrary examples are those in which the political dispute remains, such as North Korea, Vietnam, Iraq, Cuba, Red China, and a few others. In all of these examples, the opposing leadership was NOT defeated, either in war or in an internal power struggle. Clearly, it is not the PEOPLE who maintain the dispute, but the leadership.

Consider how history might have changed if we'd been able to "bump off" Lenin, Stalin, Hitler, Mussolini, Tojo, Kim Il Sung, Ho Chi Minh, Ayatollah Khomeini, Saddam Hussein, Moammar Khadafi, and various others, along with all of their replacements if necessary, all for a measly few million dollars, rather than the billions of dollars and millions of lives that subsequent wars cost.

But that raises an interesting question, with an even more interesting answer. "If all this is so easy, why hasn't this been done before?" I mean, wars are destructive, costly, and dangerous, so why hasn't some smart politician figured out that instead of fighting the entire country, we could just 'zero' the few bad guys on the top?

The answer is quite revealing, and strikingly "logical": If we can kill THEIR leaders, they can kill OUR leaders too. That would avoid the war, but the leadership on both sides would be dead, and guess who is making the decisions about what to do? That's right, the LEADERS!

And the leaders (both theirs and ours!) would rather see 30,000,000 ordinary people die in WWII than lose their own lives, if they can get away with it. Same in Korea, Vietnam, the Gulf War, and numerous other disputes around the globe. You can see that as long as we continue to allow leaders, both "ours" and "theirs," to decide who should die, they will ALWAYS choose the ordinary people of each country.

One reason the leaders have been able to avoid this solution is simple: While it's comparatively easy to "get away with murder," it's a lot harder to reward the person who does it, and that person is definitely taking a serious risk. (Most murders are solved based on some prior relationship between the murder and victim, or observations of witnesses who know either the murderer or the victim.)

Historically, it has been essentially impossible to adequately motivate an assassin, ensuring his safety and anonymity as well, if only because it has been impossible to PAY him in a form that nobody can trace, and to ensure the silence of all potential witnesses. Even if a person was willing to die in the act, he would want to know that the people he chooses would get the reward, but if they themselves were identified they'd be targets of revenge.

All that's changed with the advent of public-key encryption and digital cash. Now, it should be possible to announce a standing offer to all comers that a large sum of digital cash will be sent to him in an untraceable fashion should he meet certain "conditions," conditions which don't even have to include proving (or, for that matter, even claiming) that he was somehow responsible for a death.

I believe that such a system has tremendous implications for the future of freedom. Libertarians in particular (and I'm a libertarian) should pay particular attention to the fact that this system "encourages" if not an anarchist outcome, at least a minarchist (minimal government) system, because no large governmental structure could survive in its current form.

In fact, I would argue that this system would solve a potential problem, occasionally postulated, with the adoption of libertarianism in one country, surrounded by non-libertarian states. It could have reasonably been suspected that in a gradual shift to a libertarian political and economic system, remnants of a non-libertarian system such as a military would have to survive, to protect society against the threats represented by foreign states. While certainly plausible, it would have been hard for an average naive person to imagine how the country would maintain a $250 billion military budget, based on voluntary contributions.

The easy answer, of course, is that military budgets of that size would simply not happen in a libertarian society. More problematic is the question of how a country would defend itself, if it had to raise its defenses by voluntary contribution. An equally simplistic answer is that this country could probably be defended just fine on a budget 1/2 to 1/3 of the current budget. True, but that misses the point.

The real answer is even simpler. Large armies are only necessary to fight the other large armies organized by the leadership of other, non-libertarian states, presumably against the will of their citizenry. Once the problem posed by *their* leadership is solved (as well as ours; either by their own citizenry by similar anonymous contributions, or by ours), there will be no large armies to oppose.

Part 3

In the 1960's movie, "The Thomas Crown Affair," actor Steve McQueen plays a bored multi-millionaire who fights tedium by arranging well-planned high-yield bank robberies. He hires each of the robbers separately and anonymously, so that they can neither identify him nor each other. They arrive at the bank on schedule, separately but simultaneously, complete the robbery, then separate forever. He pays each robber out of his own funds, so that the money cannot be traced, and he keeps the proceeds of each robbery.

In my recent essay generally titled "Digitaliberty," or earlier "Assassination politics," I hypothesized that it should be possible to LEGALLY set up an organization which collects perfectly anonymous donations sent by members of the public, donations which instruct the organization to pay the amount to any person who correctly guesses the date of death of some named person, for example some un-favorite government employee or officeholder. The organization would total the amounts of the donations for each different named person, and publish that list (presumably on the Internet) on a daily or perhaps even an hourly basis, telling the public exactly how much a person would get for "predicting" the death of that particular target.

Moreover, that organization would accept perfectly anonymous, untraceable, encrypted "predictions" by various means, such as the Internet (probably through chains of encrypted anonymous remailers), U.S. mail, courier, or any number of other means. Those predictions would contain two parts: A small amount of untraceable "digital cash," inside the outer "digital envelope," to ensure that the "predictor" can't economically just randomly choose dates and names, and an inner encrypted data packet which is encrypted so that even the organization itself cannot decrypt it. That data packet would contain the name of the person whose death is predicted, and the date it is to happen.

This encrypted packet could also be published, still encrypted, on the Internet, so as to be able to prove to the world, later, that SOMEBODY made that prediction before it happened, and was willing to "put money on it" by including it outside the inner encrypted "envelope." The "predictor" would always lose the outer digital cash; he would only earn the reward if his (still-secret) prediction later became true. If, later on, that prediction came true, the "lucky" predictor would transmit the decrypt key to the organization, untraceably, which would apply it to the encrypted packet, and discover that it works, and read the prediction made hours, days, weeks, or even months earlier. Only then would the organization, or for that matter anyone else except the predictor, know the person or the date named.

Also included in that inner encrypted digital "envelope" would be a public key, generated by the predictor for only this particular purpose: It would not be his "normal" public key, obviously, because that public key would be traceable to him. Also present in this packet the predictor has earned. (This presentation could be done indirectly, by anintermediary, to prevent a bank from being able to refuse to deal with the organization.)

Those "digital cash" codes will then be encrypted using the public key included with the original prediction, and published in a number of locations, perhaps on the Internet in a number of areas, and available by FTP to anyone who's interested. (It is assumed that this data will somehow get to the original predictor. Since it will get to "everyone" on the Internet, it will presumably be impossible to know where the predictor is.) Note, however, that only the person who sent the prediction (or somebody he's given the secret key to in the interim) can decrypt that message, and in any case only he, the person who prepared the digital cash blanks, can fully "unbind" the digital cash to make it spendable, yet absolutely untraceable. (For a much more complete explanation of how so-called "digital cash" works, I refer you to the August 1992 issue of Scientific American.)

This process sounds intricate, but it (and even some more detail I haven't described above) is all necessary to:

1. Keep the donors, as well as the predictors, absolutely anonymous, not only to the public and each other, but also to the organization itself, either before or after the prediction comes true.

2. Ensure that neither the organization, nor the donors, nor the public, is aware of the contents of the "prediction" unless and until it later becomes true. (This ensures that none of the other participants can be "guilty" of knowing this, before it happens.)

3. Prove to the donors (including potential future predictors), the organization, and the public that indeed, somebody predicted a particular death on a particular date, before it actually happened.

4. Prove to the donors and the public (including potential future predictors) that the amount of money promised was actually paid to whoever made the prediction that later came true. This is important, obviously, because you don't want any potential predictor to doubt whether he'll get the money if he makes a successful prediction, and you don't want any potential donor to doubt that his money is actually going to go to a successful predictor.

5. Prevent the organization and the donors and the public from knowing, for sure, whether the predictor actually had anything to do with the death predicted. This is true even if (hypothetically) somebody is later caught and convicted of a murder, which was the subject of a successful "prediction": Even after identifying the murderer through other means, it will be impossible for anyone to know if the murderer and the predictor were the same person.

6. Allow the predictor, if he so chooses, to "gift" the reward (possibly quite anonymously) to any other person, one perhaps totally unaware of the source of the money, without anyone else knowing of this.

Even the named "target" (the "victim") is also assured of something: He his best "friend," could collect the reward, absolutely anonymously, should they "predict" his death correctly. At that point, he will have no friends.

This may represent the ultimate in compartmentalization of information: Nobody knows more than he needs to, to play his part in the whole arrangement. Nobody can turn anyone else in, or make a mistake that identifies the other participants. Yet everyone can verify that the "game" is played "fairly": The predictor gets his money, as the donors desire. Potential future predictors are satisfied (in a mathematically provable fashion) that all previous successful predictors were paid their full rewards, in a manner that can't possibly be traced. The members of the public are assured that, if they choose to make a donation, it will be used as promised. This leads me to a bold assertion: I claim that, aside from the practical difficulty and perhaps, theoretical impossibility of identifying either the donors or the predictor, it is very likely that none of the participants, with the (understandable) hypothetical exception of a "predictor" who happens to know that he is also a murderer, could actually be considered "guilty" of any violation of black-letter law. Furthermore, none of the participants, including the central organization, is aware, either before or after the "prediction" comes true, that any other participant was actually in violation of any law, or for that matter would even know (except by watching the news) that any crime had actually been committed.

After all, the donors are merely offering gifts to a person who makes a successful prediction, not for any presumed responsibility in a killing, and the payment would occur even if no crime occurred. The organization is merely coordinating it all, but again isolating itself so that it cannot know from whom the money comes, or to whom the money eventually is given, or whether a crime was even committed. (Hypothetically, the "predictor" could actually be the "victim," who decides to kill himself and "predict" this, giving the proceeds of the reward to his chosen beneficiary, perhaps a relative or friend. Ironically, this might be the best revenge he can muster, "cheating the hangman," as it were.)

In fact, the organization could further shield itself by adopting a stated policy that no convicted (or, for that matter, even SUSPECTED) killers could receive the payment of a reward. However, since the recipient of the reward is by definition unidentified and untraceable even in theory, this would be a rather hollow assurance since it has no way to prevent such a payment from being made to someone responsible.

Part 4

In part 3, I claimed that an organization could quite legally operate, assisted by encryption, international data networking, and untraceable digital cash, in a way that would (indirectly) hasten the death of named people, for instance hated government employees and officeholders. I won't attempt to "prove" this, for reasons that I think will be obvious. First, even if such an operation were indeed "legal," that fact alone would not stop its opponents from wanting to shut it down. However, there is also another way of looking at it: If this system works as I expect it would, even its claimed "illegality" would be irrelevant, because it could operate over international borders and beyond the legal reach of any law-abiding government.

Perhaps the most telling fact, however, is that if this system was as effective as it appears it would be, no prosecutor would dare file charges against any participant, and no judge would hear the case, because no matter how long the existing list of "targets," there would always be room for one or two more. Any potential user of this system would recognize that an assault on this system represents a threat to its future availability, and would act accordingly by donating money to target anyone trying to shut it down.

Even so, I think I should address two charges which have been made, apparently quite simplistically, claiming that an implementation of this idea would violate the law. Specifically: "Conspiracy to commit murder" and "misprision of felony."

As I understand it, in order to have a "conspiracy" from a criminal standpoint, it is necessary to have at least two people agree to commit a crime, and have some overt act in furtherance of that crime.

Well, this charge already "strikes out" because in the plan I described, none of the participants *agrees* with ANYONE to commit a crime. None of the participants even informs anyone else that he will be committing a crime, whether before or after the fact. In fact, the only crime appears (hypothetically; this assumes that a crime was actually committed) to be a murder committed by a single individual, a crime unknown to the other participants, with his identity similarly unknown.

Remember, the "prediction" originally sent in by the predictor was fully encrypted, so that the organization (or anyone else, for that matter) would be unable to figure out the identity of the person whose death was predicted, or the date on which it was predicted to occur. Thus, the organization is incapable of "agreeing" with such a thing, and likewise the donors as well. Only if the prediction later came true would the decrypt key arrive, and only then would the organization (and the public) be made aware of the contents. Even then, it's only a "prediction," so even then, nobody is actually aware of any crime which can be associated with the predictor.

"Misprision of Felony"

This crime, sort of a diluted form of "accessory before and/or after the fact," was claimed to qualify by "Tim of Angle," who subsequent to my answer to him on this subject has totally failed to support his initial claim. (A recent curiosity is that this crime is one that has been charged against Michael Fortier, the person who claims he helped OKC bombing suspect Tim McVeigh "case the joint" at the Federal building.)

I include it here, nevertheless, because his simplistic (and un-careful) reading of my idea led him to perhaps the "closest" law that one might allege that the participants would have broken. Tim claimed: No. That's called "misprision of felony" and makes you an accessory before the fact. Arguably, under the felony murder rule you could get TOA> capital punishment in a state that has such.

However, I did a little library research, checking *Black's Law Dictionary*. Here is the entry for this item: "Misprision of felony. The offense of concealing a felony committed by another, but without such previous concert with or subsequent assistance to the felon as would make the party concealing an accessory before or after the fact. *United States v. Perlstein*, C.C.A.N.J., 126 F.2d 789, 798. Elements of the crime are that the principal committed and completed the felony alleged, that the defendant had full knowledge of that fact, that the defendant failed to notify the authorities, and that defendant took an affirmative step to conceal the crime. *U.S. v. Ciambrone*, C.A. Nev., 750 F.2d 1416, 1417. Whoever, having knowledge of the actual commission of a felony recognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, is guilty of the federal crime of misprision of felony. 18 U.S.C.A 4." See also Obstructing Justice in *Black's Law Dictionary*.

The only "element" of this crime which is arguably satisfied is the first: Some person other than the defendant for "misprision of felony") committed a crime. The second element fails miserably: "...that the defendant had full knowledge of that fact... " My previous commentary makes it clear that far from "full knowledge of that fact," other participants are carefully prevented from having ANY "knowledge of that fact." The third element, "..that the defendant failed to notify the authorities..." is also essentially non-existent: No other participants have any information as to the identity of a predictor, or his location, or for that matter whether he has had any involvement in any sort of crime. In fact, it would be possible for each of the other participants to deliver (anonymously, presumably) copies of all correspondence they have sent, to the police or other agency, and that correspondence would not help the authorities even slightly to identify a criminal or even necessarily a crime.

In fact, normal operation of this organization would be to publicize "all" correspondence it receives, in order to provide feedback to the public to assure them that all participants are fulfilling their promises and receiving their rewards. This publication would presumably find its way to the police, or it could even be mailed to them on a "fail[ing] to notify authorities." Nevertheless, none of this material could help any authorities with their investigations, to their dismay.

The fourth and last element of the crime of "misprision of felony", "...and that defendant took an affirmative step to conceal the crime," would totally fail. The organization would not " conceal" the crime. In fact, it will have no ability to do anything to the contrary, if for no other reason that it *has* no knowledge of the crime! And as described above, it would carefully avoid having access to any information that could help solve the crime, and thus it would escape any obligations along these lines.

Summary:

In hindsight, it is not surprising that such an organization could operate legally within the U.S., although at least initially not without political opposition. First, this is at least nominally supposed to be a "free country," which should mean that police and other authorities aren't able to punish behavior just because they don't like it.

Secondly, it is obvious that most laws today were originally written during an era in which laws assumed that "conspirators" at least knew each other, had met each other, could identify each other, or had (at least!) talked to each other. On the contrary, in my scenario none of the participants even know on what continent any of the others reside, let alone their country, city, or street. They don't know what they look like, sound like, or for that matter even "type like": None of their prose, save a few sparse "predictions," ever gets communicated to anyone else, so even text-comparison programs would fail to "target" anyone.

Equally surprising (to those who originally wrote the laws against "conspiracy") would be "Person A's" ability to satisfy himself that "Person B" deserves the award, without knowing that "Person B" is (or is not) actually responsible for a particular death.

Part 5

In the previous four notes on the subject of Digitaliberty, I've suggested that this concept (collecting anonymous donations to, in effect, "purchase" the death of an un-favorite government employee) would force a dramatic reduction of the size of government at all levels, as well as achieving what will probably be a "minarchist" (minimal government) state at a very rapid rate. Furthermore, I pointed out that I thought that this effect would not merely affect a single country or continent, but might in fact spread through all countries essentially simultaneously.

But in addition to such (apparently) grandiose claims, it occurs to me that there must be other changes to society that would simultaneously occur with the adoption of such a system. After all, a simplistic view of my idea might lead one to the conclusion that there would be almost no governmental structure left after society had been transformed. Since our current "criminal justice system" today is based totally on the concept of "big government," this would lead a naive person to wonder how concepts such as "justice," "fairness," "order," and for that matter protection of individual rights can be accomplished in such a society.

Indeed, one common theme I've seen in criticisms of my idea is the fear that this system would lead to "anarchy." The funny thing about this objection is that, technically, this could easily be true. But "anarchy" in real life may not resemble anything like the "anarchy" these people claim to fear, which leads me to respond with a quote whose origin I don't quite remember:

"Anarchy is not lack of order. Anarchy is lack of ORDERS."

People presumably will continue to live their lives in a calm, ordered manner. Or, at least as calm and ordered as they WANT to. It won't be "wild in the streets," and they won't bring cannibalism back as a national sport, or anything like that.

It occurs to me that probably one of the best ways to demonstrate that my idea, "assassination politics" (perhaps ineptly named, in view of the fact that its application is far greater than mere politics), would not result in "lack of order" is to show that most if not all of the DESIRABLE functions of the current so-called "criminal justice system" will be performed after its adoption. This is true even if they will be accomplished through wholly different methods and, conceivably, in entirely different ways than the current system does.

I should probably first point out that it is not my intention to re-write the book of minarchist theory. I would imagine that over the years, there has been much written about how individuals and societies would function absent a strong central government, and much of that writing is probably far more detailed and well-thought-out than anything I'll describe here.

One reason that ALMOST ANY "criminal justice system" would be better and more effective than the one we currently possess is that, contrary to the image that officialdom would try to push, anyone whose job depends on "crime" has a strong vested interest in *maintaining* a high level of crime, not eliminating it. After all, a terrorized society is one that is willing to hire many cops and jailers and judges and lawyers, and to pay them high salaries. A safe, secure society is not willing to put up with that. The "ideal" situation, from the limited and self-interested standpoint of the police and jailers, is one that maximizes the number of people in prison, yet leaves most of the really dangerous criminals out in the streets, in order to maintain justification for the system. That seems to be exactly the situation we have today, which is not surprising when you consider that the police have had an unusually high level of input into the "system" for many decades.

The first effect of my idea would be, I think, to generally eliminate prohibitions against acts which have no victims, or "victimless crimes." Classic examples are laws against drug sales and use, gambling, prostitution, pornography, etc. That's because the average (unpropagandized) individual will have very little concern or sympathy for punishing an act which does not have a clear victim. Without a large, central government to push the propaganda, the public will view these acts as certainly not "criminal," even if still regarded as generally undesirable by a substantial minority for a few years. Once you get rid of such laws, the price of currently illegal drugs would drop dramatically, probably by a factor of 100. Crime caused by the need to get money to pay for these drugs would drop drastically, even if you assume that drug usage increased due to the lowering of the price.

Despite this massive reduction in crime, perhaps as much as 90%, the average person is still going to want to know what "my system" would do about the residual, "real" crime rate. You know, murder, rape, robbery, burglary, and all that. Well, in the spirit of the idea, a simplistic interpretation would suggest that an individual could target the criminal who victimizes him, which would put an end to that criminal career.

Some might object, pointing out that the criminal is only identified in a minority of crimes. That objection is technically correct, but it's also a bit misleading. The truth is that the vast majority of "victim"-type crime is committed by a relatively tiny fraction of the population who are repeat criminals. It isn't necessary to identify For example, even if the probability of a car thief getting caught, per theft, is only 5%, there is at least a 40% probability of getting caught after 10 thefts, and a 65% chance after 20 thefts. A smart car-theft victim would be happy to donate money targeting ANY discovered car-thief, not necessarily just the one who victimized him.

The average car-owner would be wise to offer such donations occasionally, as "insurance" against the possibility of his being victimized someday: An average donation of 1 cent per day per car would constitute $10,000 per day for a typical city of 1 million cars. Assuming that amount is far more than enough to get a typical car thief's "friends" to "off" him, there is simply no way that a substantial car-theft subculture could possibly be maintained.

Another alternative is that insurance companies would probably get into the act: Since they are going to be the financial victims of thefts of their insured's property, it is reasonable to suppose that they would be particularly inclined to deter such theft. It is conceivable that current-day insurance companies would transmogrify themselves into investigation/deterrence agencies, while maintaining their insurance role, in view of the fact that they have the most to lose. This is particularly true because if "assassination politics" (as applied to criminals and crime) comes about, they could then actually DO SOMETHING about the problem, rather than merely reporting on the statistics to their customers and stockholders.

Such companies would also have a strong motivation to provide a workable system of rewards for solving crimes and identifying criminals, rewards that (naturally enough!) can be given out totally anonymously.

While I would like to talk about the other advantage of this new kind of justice, the fact that politicians and other government employees would no longer have de-facto immunity in most cases, the reality is that since we would no longer HAVE "politicians and other government employees," to mention that advantage would be redundant.

The principle is valid, however: In today's system, you can have people known to be guilty of crimes, but not prosecuted because they are part of "the system." Classic examples would be heroes of the right (Oliver North) and heroes of the left (Jim Wright) who either escape prosecution or conviction for "political" or "bureaucratic" reasons. With "assassination politics" that would simply never happen.

Part 6

A frequent initial belief among people who have recently heard of my "assassination politics" idea is the fear that this system will somehow be "out of control": It would end up causing the death of ordinary, "undeserving" people.

This system, however, will not be without its own kind of "control. "Not a centralized control, decidable by a single individual, but a decentralized system in which everyone gets an implicit "vote." A good analogy might be to consider a society in which everyone's house thermostat is controlled to operate at a temperature which is set for the entire country. Each person's control input is taken as a "vote," whether to get hotter, colder, or to stay the same temperature. The central control computer adjusts the national setpoint temperature in order to equalize the number of people who want the temperature colder and hotter. Each house is at the same, nationally set temperature, however. Clearly, no one individual is in control of the setting. Nevertheless, I think it would be generally agreed that this system would never produce a REALLY "off the wall" temperature setting, simply because so many people's inputs are used to determine the output. Sure, if a group of 10,000 kids decided (assisted by the Internet) together to screw with the system, and they all set their houses' thermostat inputs to "hotter," they could SLIGHTLY increase the overall setting, but since there are probably about 100 million separate dwellings in the U.S., their fiddlings will be drowned out by the vast majority of the population's desires. Is this system "out of control"? True, it is out of the "control" of any single individual, but nevertheless it is well within the control of the population as a whole.

It turns out that "assassination politics" actually has a rather similar control mechanism to the one I've described above. First, I've pointed out that if I were to operate a centralized system such as this, I'd only accept donations naming people who are in violation of the "Non-Initiation Of Force Principle" (NIOFP), well known to libertarians. By this standard, government employees (who have accepted paychecks paid for with funds stolen from citizenry by taxes) and criminals whose crimes actually had a victim would be included. Let's call this hypothetical organization "Organization A," or OrgA for short.

True, somebody else might be a little less scrupulous, accepting donations for the termination of ANYBODY regardless of whether he "deserves" his fate (call them "Organization B," or OrgB, for short.) Most potential donors (who, I suggest, would have "typical" levels of scruples) would see that if they patronize OrgB, their interests wouldn't be protected. For example, OrgB (if it survives and thrives) might later come back to target them, because of some other donor. OrgA would not. Naturally, our "ethical" donors don't want this, so they would choose to give their donation to the most "ethical" organization that will accept it. This maximizes the donors' benefit, and minimizes the potential harm.

Since BOTH organizations will accept donations for "deserving" victims, while only OrgB will accept them for "just anybody," it is reasonable to conclude that (capitalism being what it is) OrgB's rates (the percentage of the price it keeps as profit) can be and will be higher for its donations (that's because there is less competition in its area of specialization.) Thus, it would be more economical to target "deserving" people through OrgA , and thus donors will be drawn to it. In addition, OrgA will become larger, more credible, believable and trustworthy, and more potential "guessers" (assassins?) will "work" its system, and for lower average potential payments (all else being equal.) Even so, and ironically, the average donation level for people listed by OrgA would likely be higher, since (if we assume these are "deserving" people) more people will be contributing towards their demise.

After all, if a potential donor wants to "hit" some government bigwig, there will be PLENTY of other donors to share the cost with. Millions of donations of $1 to $10 each would be common and quite economical. On the other hand, if you just selected a target out of the telephone directory, an "undeserving" target, you'll probably be the only person wanting to see him dead, which means that you'll probably have to foot the whole bill of perhaps $5K to $10K if you want to see any "action. " Add to that OrgB 's "cut," which will probably be 50%, and you're talking $10K to $20K. I contend that the likelihood of this kind of thing actually happening will be quite low, for "undeserving victims."

Now, the die-hards among you will probably object to the fact that even this tiny residual possibility is left. But consider: Even *today* it would be quite "possible" for you to pick a name randomly out of a list, find him and kill him yourself. Does this frequently happen? Apparently not. For just one thing, there's no real motive. Unless you can show that the application of "assassination politics" would dramatically increase the likelihood of such incidents, I suggest that this "problem" will likely not be a problem after all.

For a while, I thought that the "lack of a motive" protection was momentarily overturned by a hypothetical: I thought, suppose a person used this system as part of a sophisticated extortion scheme, in which he sends an anonymous message to some rich character, saying something like "pay me a zillion dollars anonymously, or I put out a digital contract on you." For a while, this one had me stumped. Then, I realized that an essential element in this whole play was missing: If this could be done ONCE, it could be done a dozen times. And the victim of such an extortion scheme has no assurance that it won't happen again, even if he pays off, so ironically he has no motivation to pay off the extortion. Think about it: The only reason to make the payment is to remove the threat. If making the payment can't guarantee to the target that the threat is removed, he has no reason to make the payment. And if the target has no reason to make the payment, the extortionist has no reason to make the threat!

Another, related (and equally simplistic) fear is that political minorities will be preferentially targeted. For example, when I pointed out that "establishment" political leaders would probably "go" quite quickly, one wag suggested to me that "libertarian leaders" could likewise be targeted. Such a suggestion reflects a serious misunderstanding of political philosophy, and libertarians in particular: I consider it obvious (to me, at least) that libertarians NEED no leaders. (You don't need leaders if you don't want to control a population, or achieve political power. The only reason libertarians "need" leaders today is to take places in the government and (then) to shut it down.) And if my idea is implemented, "libertarian leaders" represent no more of a threat to anyone than the average libertarian citizen.

Fully recognizing this, another (and far more credible) person thought a while, and in a proud revelation suggested that one way that the establishment would "fight back" is to convert to a government that is based on fully decentralized authority, as opposed to the leader-centric system we have today. Such a system could not be attacked by killing individual people, any more than you can kill a tree by pulling off a single leaf. His "solution" was, in effect, to totally disband the current government and turn it over to the public at large, where it highly de-centralized system that is not controlled by a tiny fraction of the population in a structure called a "government," essentially identical to his idea. So in effect, the only way the government can survive is to totally surrender. And once it surrenders, the people win. And in practice, it will have no alternative.

Will this idea be "out of control"? To a great extent, that depends on what your definition of the word "control." I have come to believe that "assassination politics" is a political Rorschach (ink-blot) test: What you think of it is strongly related to your political philosophy.

Part 7

Dear libertarian Friend,

I very much understand the concerns you voiced about my idea which I call, "Assassination Politics," because this essay is nothing if it is not radical and extreme. I wrote it, in the middle of last year, partly because I think libertarianism and libertarians in particular need to address what is, if not a contradiction," is at least an intolerable reality: On the one hand, we are told not to initiate aggression, but on the other we are aggressed against by the government every time it collects a tax.

I much appreciate the way some people I know have "dropped out" of the system, and the guts that such a tactic requires. But that's the problem, I think: Only those with the "guts" do it, which gives the government fewer targets so that it can spend more time attacking the few who oppose it. The reality is that the government STILL collects taxes, and it STILL uses that money to violate our rights. We all know that's wrong.

My position is quite simple: If tax collection constitutes aggression, then anyone doing it or assisting in the effort or benefiting from the proceeds thereof is a criminal. This is quite analogous to current law which prosecutes co-conspirators. While I am not holding out "current law" as some sort of gold-standard of reasonableness that we must always accept, on the other hand I think it's plausible to use it to show that once we have come to the conclusion that taxation is theft, the prescription follows directly by a form of reasoning allegedly acceptable to society: It is reasonable to "attack the attackers" and their co-conspirators, and everyone who is employed by the government is thus a co-conspirator, even if he is not directly involved in the collection of those taxes. That's because he IS involved in *benefiting* from the proceeds of these taxes, and he presumably provides a certain level of "backup" to the young thugs that governmental organizations often hire.

I realize, and you should too, that the "non-aggression principle" says nothing about the EXTENT of the self-defense/retaliation that one might reasonably employ in defending one's own rights: In a sense, that sounds like an omission because it at least suggests that a person might "unreasonably" defend himself with lethal force when far less drastic means might normally be called for. For what it's worth, I think most people will behave responsibly. But I think it is pretty straightforward to argue that whatever means are necessary to stop the attack, are reasonable given the terms of the non-aggression principle: If a given means are known to be inadequate to actually stop the attack, then further and more serious means are reasonable and called-for.

To set up a reasonable analogy, if I'm walking down the canonical "dark alley" and am accosted by a man wielding a knife threatening me with it, it is presumably reasonable for me to pull a gun and threaten back, or possibly take the encounter to the final conclusion of gunfire. Even if I should choose to hold my fire and test to determine whether my actions deterred him, I can't see that this possibility binds me morally. And should he advance, despite the gun, as if to attack, I should feel no remorse in shooting him and taking myself out of danger. If you accept the premises so far, you apparently accept the principle that escalation of the self-defense/retaliation is reasonable as long as if the current level of returned counter-threat is inadequate to stop the aggression initiated by the other party. To believe otherwise is to believe that ultimately, you are obligated to accept a certain high level of aggression simply because you do not have the resources (yet) to resist it. I totally reject this concept, as I hope you would.

So if, hypothetically, I could have an anonymous conversation with a hard-nosed government employee, and asked him, "If I killed one of your agents, would you stop trying to collect that tax from me," his predictable reaction would be, "no, we would continue to try to collect that tax." In fact, he would probably hasten to add that he would try to have me prosecuted for murder, as well! If I were to ask if killing ten agents would stop them, again they would presumably say that this would not change their actions.

The conclusion is, to me, obvious: Clearly, there is no practical limit to the amount of self-defense that I would need to protect my assets from the government tax collector, and to actually stop the theft, so I suggest that logic requires that I be morally and ethically allowed (under libertarian principles) to use whatever level of self-defense I choose.

You raised another objection, that quite frankly I believe is invalid. I believe you implied that until a specific level of escalation is reached (such as the Feds showing up on your doorstep, etc) then it is not legitimate to defend oneself. Delicately, I must disagree. As we all well know, government ultimately operates primarily not on actual, applied force, but simply the threat of future force if you do not comply. True, there are people who have decided to call the government's bluff and simply drop out, but the reality is that this is not practical for most individuals today. This is no accident: The government makes it difficult to drop out, because they extort the cooperation of banks and potential employers and others with which you would otherwise be able to freely contract. In any case, I fail to see how not "dropping out" makes one somehow morally obligated to pay a tax (or tolerate the collection of one). I trust you did not inadvertently mean to suggest this.

The reason, morally, we are entitled to shoot the mugger if he waves the knife in our face is that he has threatened us with harm, in this case to our lives, but the threat the government represents to the average citizen (loss of one's entire assets) is just as real, albeit somewhat different. Since government is a past reality, and a present reality, and has the immediate prospects of being a future reality as well, I sincerely believe that the average citizen can legitimately consider himself CONTINUOUSLY threatened. The aggression has already occurred, in continuously occurring, and has every prospect of continuing to occur. If anything would justify fighting back, this would.

To continue the analogy, if you've been repeatedly mugged by the same guy down the same dark alley for each day of last month, that DOES NOT mean that you've somehow consented to the situation, or that your rights to your assets have somehow been waived. With my "Assassination Politics" essay, I simply proposed that we (as libertarians as well as being ordinary citizens) begin to treat aggression by government as being essentially equivalent to aggression by muggers, rapists, robbers, and murderers, and view their acts as a continuing series of aggressions. Seen this way, it should not be necessary to wait for their NEXT aggression; they will have always have been aggressing and they will always BE aggressing, again and again, until they are stopped for good.

At that point, the question shifted to one of practicality: Sure, theoretically we might morally have the "right" to protect ourselves with lethal force, but if they have any reputation at all, government agents have a habit of showing up in large numbers when they actually apply direct force. To take a position that you can only defend yourself when *they've* chosen the "where" and "when" of the confrontation is downright suicidal, and I hope you understand that I would consider any such restriction to be highly unfair and totally impractical. Understand, too, that the reason we're still stuck under the thumb of the government is that to the extent it's true, "we've" been playing by THEIR rules, not by our own. By our own rules, THEY are the aggressors and we should be able to treat them accordingly, on our own terms, at our own convenience, whenever we choose, especially when we feel the odds are on our side.

I understand, obviously, that the "no initiation of aggression" principle is still valid, but please recognize that I simply don't consider it to be a valid counter-argument to "Assassination Politics," at least as applied to targets who happen to be government agents. They've "pre-aggressed," and I don't see any limit to the defenses I should be able to muster to stop that aggression completely and permanently. Not that I don't see a difference between different levels of guilt: I fully recognize that some of them are far worse than others, and I would certainly not treat a lowly Forest Service grunt in the same fashion as an ATF sniper.

Now, there is one more thing that I would hope we could get straight: As I originally "invented" this system, it occurred to me that there could be certain arguments that it needed to be "regulated" somehow; "unworthy" targets shouldn't be killed, etc. The "problem" is, what I've "invented" may (as I now believe it to be) actually a "discovery," in a sense: I now believe this kind of system was always inevitable, merely waiting for the triad of the Internet, digital cash, and good encryption in order to provide the technical underpinnings for the entire system. If that is genuinely the case, then there is no real way to control it, except by free-market principles.

It would be impossible, for example, to set up some sort of "Assassination Politics Dictator," who decides who will live and who will die, because competition in the system will always rise to supply every demand, albeit at possibly a very high price. And if you believe the maxim that "absolute power corrupts absolutely," you wouldn't want to accept any form of centralized control (even, perhaps, that of your own!), because any such control would eventually be corrupted. Most rational people recognize this, and I do too. I would not have invented a system where "Jim Bell" gets to make "all the decisions." Quite the contrary, the system I've described absolutely prevents such centralization. That, quite frankly, is the novelty and dare I say it, the beauty of this idea. I believe that it simply cannot be hijacked by centralized political control.

As I pointed out in the essay, if *I* were running one of the organizations accepting those donations and offering those prizes, I would selectively list only those targets who I am genuinely satisfied are guilty of the violation of the "non-aggression principle." But as a practical matter, there is no way that I could stop a DIFFERENT organization from being set up and operating under DIFFERENT moral and ethical principles, especially if it operated anonymously, as I anticipate the "Assassination Politics"-type systems will be. Thus, I'm forced to accept the reality that I can't dictate a "strongly limited" system that would "guarantee" no "unjustified" deaths: I can merely control my little piece of the earth and not assist in the abuse of others. I genuinely believe, however, that the operation of this system would be a vast improvement over the status quo.

This, I argue, is somewhat analogous to an argument that we should be entitled to own firearms, despite the fact that SOME people will use them wrongly/immorally/illegally. The ownership is a right even though it may ultimately allow or enable an abuse that you consider wrong and punishable. I consider the truth of such an argument to be obvious and correct, and I know you would too.

I realize that this lacks the crisp certitude of safety which would be reassuring to the average, "pre-libertarian" individual. But you are not the "average individual" and I trust that as long-time libertarians you will recognize rights must exist even given the hypothetical possibility that somebody may eventually abuse them.

I do not know whether I "invented" or "discovered" this system; perhaps it's a little of both. I do genuinely believe that this system, or one like it, is as close to being technologically inevitable as was the invention of firearms once the material we now know as "gunpowder" was invented. I think it's on the way, regardless of what we do to stop it. Perhaps more than anyone else on the face of this planet, this notion has filled me, sequentially and then simultaneously, with awe, astonishment, joy, terror, and finally, relief.

Awe, that a system could be produced by a handful of people that would rid the world of the scourge of war, nuclear weapons, governments, and taxes. Astonishment, at my realization that once started, it would cover the entire globe inexorably, erasing dictatorships both fascistic and communistic, monarchies, and even so-called "democracies," which as a general rule today are really just the facade of government by the special interests. Joy, that it would eliminate all war, and force the dismantling not only of all nuclear weapons, but also all militaries, making them not merely redundant but also considered universally dangerous, leaving their "owners" no choice but to dismantle them, and in fact no reason to KEEP them!

Terror, too, because this system may just change almost EVERYTHING how we think about our current society, and even more for myself personally, the knowledge that there may some day be a large body of wealthy people who are thrown off their current positions of control of the world's governments, and the very-real possibility that they may look for a "villain" to blame for their downfall. They will find one, in me, and at that time they will have the money and (thanks to me, at least partially) the means to see their revenge. But I would not have published this essay if I had been unwilling to accept the risk.

Finally, relief. Maybe I'm a bit premature to say it, but I'm satisfied we *will* be free. I'm convinced there is no alternative. It may feel like a roller-coaster ride on the way there, but as of today I think our destination is certain. Please understand, we *will* be free.

Your libertarian friend,

Jim Bell

jimbell@pacifier.com

Something is going to happen... Something... Wonderful!

Part 8

The following article appeared in the Sunday, February 4, 1996 issue of *Asahi Evening News*, in an article written by columnist Paul Maxwell, page 6. He writes a regular column about the Internet for this newspaper.

"Networks: Paul Maxwell"

"Dial Internet for murder"

'The first thing we do, let's kill all the lawyers." (Shakespeare, Henry VI).

A startling and controversial idea has surfaced on the Internet recently--fear with me for a moment while I explain it. It is based on two technological developments: digital cash and encryption software.

Briefly, digital cash is a system for transferring funds from one person to another on the Net. For this system to be as good as cash, the transactions must be capable of being conducted anonymously, just like in real life. (You go into the Seven-Eleven, buy a Cafe Latte, and nobody knows your name or your credit history. The purchase is not recorded in a database of your consumer preferences.)

Several competing schemes for digital cash have been launched, but the one that eventually gains universal acceptance will surely have this anonymity feature.

The second innovation is a kind of software called public-key encryption. It allows you to send a file or an email message that is "locked" in such a way that it can only be opened by the intended recipient. The recipient, however, cannot open it until given a "key." This "key" may then be used to encrypt a return message that can only be opened by the original sender.

Freelance visionary and tinkerer Jim Bell has been following both of these developments for the past few years. Recently, he asked himself a couple of tough questions: "How can we translate the freedom afforded by the Internet to ordinary life?" How can we keep government from banning encryption, digital cash, and other systems that will improve our freedom?"

Suddenly, Bell had a revolutionary idea. ("Revolutionary" is the word he uses, and it fits.) You and me--the little guys, the ordinary working people of the world--could get together, all pitch in, and pay to have every rotten scoundrel in politics assassinated. And we could do it legally. Sort of. Bell imagined an organization that would award "a cash prize to somebody who correctly 'predicted' the death of one of a list of violators of rights, usually either government employees, officeholders, or appointees. It could ask for anonymous contributions from the public, and individuals would be able to send those contributions using digital cash."

He explains that "using modern methods of public-key encryption and anonymous digital cash, it would be possible to make such awards in such a way so that nobody knows who is getting awarded the money, only that the award is being given. Even the organization itself would have no information that could help the authorities find the person responsible for the prediction, let alone the one who caused the death. "Are you following this? Let's say that we, the public, decide we've finally had enough of [insert name of villain]. Ten dollars from me, ten from you--suddenly there's a million dollars in a fund. The money will go to the first person who can "predict" the date, time, and circumstances of the villain's death. Obviously, this information is only known in advance by the assassin.

He sends an anonymous, "locked" message. He kills the villain. He sends the "key" to the message. He has, without ever revealing his identity, "correctly predicted" the murder. The "key" that he has provided is then used to "lock the award money in a file that is then publicly posted on the Internet. Only the person who originated the key may open the file and claim the digital cash.

In other words, public anger could finance cash awards for assassinations. The organization that collected the money and announced a list of possible targets would never know about a crime in advance, and would never know the identity or whereabouts of a criminal. It would not technically be guilty of conspiracy or complicity.

Jim Bell has thought about this a lot, and feels that the idea is technically feasible, practical, even foolproof. Suppose for a moment he's right? What are the implications?

World leaders live with the threat of assassination every day of their lives. But at the local level, this could really have an impact. And the "target" list wouldn't necessarily to politicians--any offensive public personality would be fair game. Picture yourself a year from now, sitting around with friends. Somebody says, "Remember when Juice Newton got whacked?" And you say, "Yeah--best ten bucks I ever spent."

Satisfying as it might be to declare war on asinine pop singers, Bell has a more civic-minded suggestion: Let's kill all the car thieves. He reasons that a very small number of career criminals are responsible for nearly all car thefts. If one million car owners in a given metropolitan area contributed just four dollars a year, it would create $10,000 a day in "prize money" for the "predictor" of any car thief's death.

"Assuming that amount is far more than enough to get a typical car thief's 'friends' to 'off' him," he writes, "there is simply no way that a substantial car-theft subculture could possibly be maintained."

Jim as high hopes for his plan--he thinks it could eventually lead to the end of political tyranny. But if you don't like this idea, he has others. In a recent email exchange, I asked what he was doing now.

"I recommend that you rent the movie, "The Day the Earth Stood Still.," he answered. "I'm working on a similar project."

Part 9

by Jim Bell, February 27, 1996

For about a year I have been considering the implications of "Assassination Politics," and for more than six months I've been sharing the subject and my musings with you, the interested reader. I've also been debating the issue with all comers, a self-selected bunch who range from enthusiastic proponents to clueless critics. Ironically, some of you have even chided me for "wasting time" with some of the less perceptive among my numerous "opponents." In defense, my response has always been that when I respond to a person, I do it not primarily for his benefit, but for others who might be fence-sitting and are waiting to see if my idea will break down anywhere.

If there is anything which has fascinated me as much as the original idea, it is this vast and dramatic disparity between these various responses. It's been called everything from "a work of genius" to "atrocious," and probably much worse! Clearly, there must be a fundamental, social issue here that needs to be resolved.

While nobody has quite yet said it in those terms, I'm sure that more than one of you have probably wanted to react to my prose with the line, "See a shrink!" [American slang for a psychiatrist, for the international readers out there.] Well, in a sense that's exactly what I did, but the "shrink" I "saw" had been dead for over five decades: Sigmund Freud. Much to my surprise, I was handed a copy of a book, *Introduction to Great Books* (ISBN 0-945159-97-8) which contained (page 7) a letter from Freud to Albert Einstein. On page 6, there is an introduction, describing the reason for this communication. It says:

"In 1932, the League of Nations asked Albert Einstein to choose a problem of interest to him and to exchange views with someone about it. Einstein chose "Is there any way of delivering mankind from the menace of war?" as his problem and Sigmund Freud as his correspondent. In his letter to Freud, Einstein said that one way of eliminating war was to establish a supranational organization with the authority to settle disputes between nation as and power to enforce its decisions. But Einstein acknowledged that this solution dealt only with the administrative aspect of the problem, and that international security could never be achieved until more was known about human psychology. Must right always be supported by might? Was everyone susceptible to feelings of hate and destructiveness? It was to these questions Freud addressed himself in his reply."

Interestingly enough, when I first started thinking about the idea that I would later term "Assassination Politics," I was not intending to design a system that had the capability to eliminate war and militaries. What I was targeting, primarily, was political tyranny. By my standards, that included not merely totalitarian governments but also ones that many of us would consider far more benign, in particular the Federal government of the United States of America, "my" country. Only after I had thought of the fundamental principle of allowing large numbers of citizens to do away with unwanted politicians was I "forced," by my work up to that point, to address the issue of the logical consequences of the operation of that system, which (by "traditional" ways of thinking) would leave this country without leaders, or a government, or a military, in a world with many threats. I was left with the same fundamental problem that's plagued the libertarian analysis of forming a country in a world dominated by non-libertarian states: It was not clear how such a country could defend itself from aggression if it could not force its citizens to fight.

Only then did I realize that if this system could work within a single country, it could also work worldwide, eliminating threats from outside the country as well as corrupt politicians within. And shortly thereafter, I realized that not only could this occur, such a spread was absolutely inevitable, by the very nature of modern communications across the Internet, or older technologies such as the telephone, fax, or even letters written on paper. In short, no war need ever occur again, because no dispute would country he intended to war with, obviously, but he would also draw the ire of citizens within his own country who either didn't want to pay the taxes to support a wasteful war, or lose their sons and daughters in pointless battles, or for that matter were simply opposed to participating in the aggression. Together, all these potentially-affected peoples would unite (albeit quite anonymously, even from each other) and destroy the tyrant before he had the opportunity to make the war.

I was utterly astonished. Seemingly, and without intending to do so, I had provided a solution for the "war" problem that has plagued mankind for millennia. But had I? I really don't know. I do know, however, that very few people have challenged me on this particular claim, despite what would normally appear to be its vast improbability. While some of the less perceptive critics of "Assassination Politics" have accused me of eliminating war and replace it with something that will end up being worse, it is truly amazing that more people haven't berated me for not only believing in the impossible, but also believing that the impossible is now actually inevitable!

A little more than a week ago, I was handed this book, and asked to read Freud's letter, by a person who was aware of my "little" philosophical quandary. I began to read Freud's letter in response to Einstein, having never read any other word Freud had written, and having read essentially none of the works of the giants of Philosophy. (Now, of course, I feel tremendously guilty at the omission in my education, but I've always been attracted more to the "hard sciences," like chemistry, physics, mathematics, electronics, and computers.) Since this letter was specifically on war, and the question of whether man could ever avoid it, I felt perhaps it would contain some fact or argument that would correct what was simply a might end up being right, but alternatively hoped that if wrong, I would be soon corrected. I was fearful that I was wrong, but also fearful that there would be nothing in this essay that would assist me in my analysis of the situation.

About a third of the way through Freud's letter, I had my answer. Below, I show a segment of Freud's reply, perhaps saving the whole letter for inclusion into a later part of this ongoing essay. While I could drastically oversimplify the situation and state, "Freud was wrong!," it turns out that this brief conclusion is at best highly misleading and at worst flirting with dishonesty. By far the greater part of Freud's analysis makes a great deal of sense to me, and I would say he's probably correct. But it is at one point that I believe he goes just a bit wrong, although for reasons which are entirely understandable and even predictable, given the age in which he lived. It must be remembered, for example, that Freud was born into an era where the telephone was a new invention, broadcast radio was non-existent, and newspapers were the primary means that news was communicated to the public. It would be highly unreasonable for us to have expected Freud to have anticipated developments such as the Internet, anonymous digital cash, and good public-key encryption.

In some sense, at that point, my biggest regret was that I couldn't discuss the issue with either of these two communicants, Freud having died in 1939, and Einstein in 1955, after having helped initiate research that led to the development of the atomic bomb, the weapon that for decades and even now, makes it absolutely, vitally important to eliminate the possibility of war from the world.

But I'll let Dr. Freud speak, as he spoke over sixty years ago, because he has much to say:

> "Such then, was the original state of things: domination by whoever had the greater might--domination by brute violence or by violence supported by intellect. As we know, this regime was altered in the course of evolution. There was a path that led from violence to right or law. What was that path? It is my belief that there was only one: the path which led by way of the fact that the superior strength of a single individual could be rivaled by the union of several weak ones. "L'union fait la force." [French; In union there is strength.] Violence could be broken by union, and the power of those who were united now represented law in contrast to the violence of the single individual. Thus we see that right is the might of a community. It is still violence, ready to be directed against any individual who resists it; it works by the same methods and follows the same purposes. The only real difference lies in the fact that what prevails is no longer the violence of an individual but that of a community."

[But below is where I think Freud falls into a certain degree of error, perhaps not by the standards and realities of *his* day, but those of ours. My comments are in square brackets,], and Freud's comments are quoted "". Freud continues:]

> "But in order that the transition from violence to this new right or justice may be effected, one psychological condition must be fulfilled. The union of the majority must be a stable and lasting one. If it were only brought about for the purpose of combating a single dominant individual and were dissolved after his defeat, nothing would be accomplished. The next person who though himself superior in strength would once more seek to set up a dominion by violence and the game would be repeated ad infinitum. The community must be maintained permanently, must be organized, must draw up regulations to anticipate the risk of rebellion and must institute authorities to see that those regulations--the laws-- are respected and to superintend the execution of legal acts of violence. The recognition of a community of interests such as these leads to the growth of emotional ties between the members of a united group of people--communal feelings which are the true source of its strength." [end of Freud's quote]

[Those of you who truly comprehend the idea of "Assassination Politics" will, I'm confident, understand exactly why I considered this segment of Freud's letter to be important enough to include, and will probably also recognize why I consider Freud's analysis to go wrong, albeit for comparatively minor and understandable reasons. I will address the last paragraph in greater detail, to explain what I mean. I will repeat Freud's words, and address each of his points from the standpoint of today's situation and technology.]

> "But in order that the transition from violence to this new right or justice may be effected, one psychological condition must be fulfilled. The union of the majority must be a stable and lasting one." [In a sense, Freud is absolutely correct: Whatever system is chosen to "govern" a society, it must continue to operate "forever."] Freud continues:
>
> " If it were only brought about for the purpose of combating a single dominant individual and were dissolved after his defeat, nothing would be accomplished."

[This is where the problem begins to creep in. Freud is leading up to justifying the existence of a formal government as he knew them in the 1930's, based on the continuing need for keeping the peace. The first, and I think, the most obvious problem is that Freud seems to implicitly assume that the purpose of the union will actually be fulfilled by the formation of a government. Freud, who died in 1939, didn't see what his survivors saw, a "legitimate" government in Germany having killed millions of people in the Holocaust, or many other incidents subsequent to that. And Freud, whose letter was written in 1932, was probably not aware of the slaughter of the Russian Kulaks in the late 1920's and early 1930's, or the purges which followed. Freud could have felt, generally, that the problems with a country's governance were caused either by inadequate government or simply a rare example of government gone bad. We know, to the contrary, that governments very frequently "go bad," in the sense of violating citizen's rights and abusing the power entrusted to them. Few may end up killing millions, but to assume that we must continue to tolerate governments just because they don't go quite as far as Nazi Germany would be foolish in the extreme.]

[The second problem is the implicit assumption that the long-term control he (correctly) sees MUST come from an organization like a traditional government. True, in the era in which Freud lived, that conclusion made a great deal of sense, because a well-functioning government appeared superior to none at all. And it was at least plausible that such control COULD come from a government. But as the old saying goes, "Power corrupts, and absolute power corrupts absolutely."]

[To use a house's thermostat as an analogy, but differently than I did in "Assassination Politics part 6," a person who lived in an era before automatic furnace thermostats would always conclude that a person's efforts would have to be continually directed towards maintaining an even temperature in his house, by adding fuel or limiting it, by adding more air or restricting, etc. To the extent that this manual control constitutes a "government," he will believe that this hands-on control will always be necessary. But we now live in a time where a person's time is rarely directed towards this effort, the function having been taken over by automatic thermostats which are cheap, reliable, and accurate. They are also, incidentally, essentially "uncorruptible," in the sense that they don't fail except for "understandable" reasons, and repair is cheap and easy. (And a thermostat can never be bribed, or get tired, or have its own interests at heart and begin to subvert your own commands.) Quite simply, the progress of technology has put control of temperature in the hands of an automatic, error-free system that is so reliable as to be ignorable most of the time.]

[I argue that likewise, the progress of technology would allow an automatic system to be set up, which I called "Assassination Politics" (but could probably use a more apt name, since its application extends far beyond the issue of politics) different from traditional government, a difference somewhat analogous to the difference between a person's full-time efforts and an automatic thermostat. Aside from the dramatic reduction in effort involved, an automatic system would eliminate the errors caused by inattention by the operator, such as leaving, falling asleep, or other temporary lack of concentration. These failures are somewhat analogous to the failure or misbehavior of a corruptible or indifferent or even a malicious government.]

[This makes a government like Freud saw totally unnecessary. Of course, Freud could not have anticipated the technological developments that would make an "automatic" replacement for government even possible, and thus he followed his contemporary paradigms and sought to justify the governments as they then existed.] Freud continues:

> "The next person who thought himself superior in strength would once more seek to set up a dominion by violence and the game would be repeated ad infinitum."

[This statement is correct, but I think it misses the point: Many functions of individuals and machines are never "completed", and must "be repeated ad infinitum." (The most basic example: If we are optimistic about the future of the human race, by definition reproduction and survival must be "repeated ad infinitum.") That does not mean that the mechanism which handles that need must be any more complicated that the minimum necessary to achieve the control needed. I agree that a system of long-term control is necessary; where I disagree with Freud is simply that I believe that a vastly better method of control now can potentially exist than the traditional governments that he knew. To the extent that he couldn't have anticipated the Internet, anonymous digital cash, and good encryption, he had no reason to believe that government could be "automated" and taken out of the hands of a tiny fraction of the population, a fraction which is corruptible, malicious, and self-interested. Also, by not being aware of modern technology, he is unaware how easy it has become, conceptually, for people to come together for their self-defense, if that self-defense required only a few kilobytes be sent over fiber-optic cables to a central registry. Freud's objection to an "endlessly repeating" system breaks down in this case, so his conclusion need not be considered valid.]

Freud continues:

> "The community must be maintained permanently, must be organized, must draw up regulations to anticipate the risk of rebellion and must institute authorities to see that those regulations--the laws-- are respected and to superintend the execution of legal acts of violence."

[Again, I think Freud misses the point. He refers to "the risk of rebellion," but I think he forgets that the main reason for "rebellion" is the abuse by the government then in control. (Naturally, it looks differently from the standpoint of that government!) If the latter problem could be eliminated, "rebellion" would simply never occur, for there would be no reason for it. If those that were "rebelling" were in the wrong, violating somebody's rights, then my "Assassination Politics" system would be able to take care of it. This, presumably and understandably, Freud could never have foreseen. Also, Freud does not address the question of whether or not the government which promulgates those laws is doing so in a way primarily for the benefit of the public, or those who populate the government itself. Graft was well known if Freud's time; it seems to me that he should have addressed the question of whether or not an entity called a "government" could actually achieve the benefits he claims justify the government, without being subverted by those who control it, for their own interests. If not, then there is certainly a issue to be addressed: At what point do the depredations of a parasitic government exceed its benefits? And can we find a way to do without it?] Freud continues:

> "The recognition of a community of interests such as these leads to the growth of emotional ties between the members of a united group of people--communal feelings which are the true source of its strength." [this is end of the portion of Freud's letter which I quote here.]

One of the interesting things about this statement is that it is the development of tools such as the Internet which will be eliminating the very concept of "foreign" and "foreigner." They will become artificial distinctions. There is clearly much precedent for this, from the country in which I live, America. When formed, it contained people whose primary loyalty was to their *state,* not to the Federal government as a whole. Even our civil war, from 1861 to 1865, was based on loyalty to states or regions, rather than the country as a whole. To cite just one example, myself, while I reside in the state called Washington, I've lived in a number of other states, but I don't consider myself loyal to any particular state. (Perhaps using myself as an example is misleading, because at this point I don't consider myself "loyal" to any government at all!)

In fact, later in Freud's letter, he says, "Anything that encourages the growth of emotional ties between men must operate against war." Sadly, Freud did not live to see the development of the Internet, and the massive international communication which it has already begun to foster. In *his* day, the ordinary people of one country and another rarely communicated, except perhaps for letters with relatives from "the old country" that emigrated. The idea of going to war with people from whom you get email on a daily basis is, in itself, a "foreign concept" to me, and I hope it will remain so! In that sense, Freud was very right: "Assassination Politics" active or not, it will be much harder for governments to whip up their citizens into a frenzy to kill the enemy if they can type to them every day. Frustratingly left unanswered is a question whose answer I'd like to know: Could I have convinced Freud, or Einstein, that "Assassination Politics" is not only a necessary or even an unavoidable system, but also a GOOD one? Could I convince them today, had they miraculously survived until today, aware of the last 64 years of history subsequent to their correspondence?

Jim Bell jimbell@pacifier.com

Klaatu Burada Nikto

Something is going to happen... Something...Wonderful!

Part 10: "Non-Euclidean Thinking"

by Jim Bell

An interesting communication I had recently on the subject of "Assassination Politics." My commentary is preceded with >> or nothing; the other person's commentary starts with a ">". The subject is how to actually implement this system, and my first comment notices the fact that despite my efforts, the government has not attempted to use this issue to justify some sort of crackdown on net rights, or anything like that.

I think they're actually afraid to start the debate,

I think they don't believe you're a threat.

You're probably right about this. I guess I'll have to think of something to change their minds, huh?

Remember, they have incredible >amounts of money with which to hire bright but greedy people. All they have to do is find the people running the "Guess the Death Date" lottery. They would have great incentive to apply their considerable resources to this end.

Your logic is excellent. But as strange as it may seem, there may be a different way... Let's see, how do I explain? First, a little diversion that may or may not be relevant to this subject, but initially won't appear to be so.

Somewhere around 20-25 years ago, I read some item concerning Howard Hughes, the late billionaire. It described the history of his business ventures, in fields such as aircraft ("Spruce Goose" is a well-known example) but also mentioned that Hughes Tool was (originally?) into oil-well drilling equipment.

I don't know how much you know about oil well drilling and drill bits, but they look nothing like the classic fluted drill bits common in hardware stores. Oil well drill bits consist of multiple ultra-hard carbide points mounted on rotating shafts mounted at the end of the drill "string," and these shafts must be connected to the main shaft with bearings. They roll around on the rock, not sliding, and they "spall" off pieces of rock due to enormous applied pressure.

Oil well drilling is done by lubricating the drilling operation with what is called "drilling mud," which is actually a slurry of solids in water, which is primarily used to cool the cutter and wash away the rock chips and dust produced in the operation. Now, since the rotating cutter wheels must spin on their axis, that means they have to be run on shafts with bearings installed. These bearings cannot be perfectly sealed and thus protected against rock and mud dust, and their useful lifetime is strongly limited by their quality.

And since every time they wear out the whole drill string has to be pulled from the well, that's an EXTREMELY expensive proposition for well-drillers. So it should not be surprising that these guys considered bearing quality to be very, very important. A little improvement was worth a lot of money.

"Quality", to a bearing manufacturer, is strongly related to surface hardness, and traditionally, the best bearings were (and, mostly, still are) the hardest. But there's a problem: Ultimately, a very hard circular bearing rotating on a very hard flat surface (especially if its heavily loaded) applies nearly all its for on a single point (for ball bearings) or on a single line (for roller bearings) and that eventually causes bearing failure. So there was an upper limit, generally, on how good you could get in bearings. And the hardest won. Until Hughes.

[don't go to sleep yet... it gets relevant real soon]

According to the source I read, what Hughes Tool did that made them really rich was quite simple and counter-intuitive: Rather than trying to make his bearings as HARD as you can get, he made them SOFT, very soft, "almost as soft as lead." (Which, if you know anything about metals, is very soft indeed.) The bearings deformed on their raceways, spreading out the load over a far larger area, and the resulting bearings were the best in the business. (He probably also applied a lot of research into how to avoid "metal fatigue," but that's quite another story.)

Very counter-intuitive, but he "won" precisely because he did exactly the opposite of what everyone "knew" was the proper way to go. Okay, so that explains a genius who later became a billionaire who later turned into a neurotic, or worse. "What," you will ask, "does this all have to do with Assassination Politics?"

Well, to draw an observation originally posited in an essay titled the "Libertech Project," about 7 years ago, libertarians (of all people) are "non-Euclidean thinkers." Basically, this means that we recognize that the best way to go from "point A" to "point B" is NOT NECESSARILY a straight line. And like Columbus, who sailed west in order to go east, sometimes it is necessary to sit down, and totally re-think your strategy if you're trying to accomplish some goal.

By "classical" thinking, "Assassination Politics" would have to be the best, tightest-security, more protected organization that has ever existed on the face of this planet. Just about EVERY powerful person would want to kill anybody who had anything to do with such a system. The codes would have to be unbreakable, the remailers would have to be certain, but most importantly, each and every participant would have to be perfectly anonymous to even have a prayer of pulling it off. Especially the operators of such a system. Especially them.

That's classical thinking. And that's what I thought a few months ago. I thought, "it's do-able, but it's gonna be a lot of work!"

But let's suppose, for a moment, that somebody "pulls a Hughes." Rather than trying to make the hardest bearings in the world, why doesn't somebody try to make the softest? Rather than trying their darndest to stay anonymous, or wait and let somebody else implement this system, why not just "let it all hang out," (as the saying went in the 1960's) and publicly announce that they're implementing this system, come hell or high water, and invite anyone who wants to participate to help form what will be the LAST revolution on earth, the one that'll take down ALL the governments.

This sounds crazy, right? I mean, who wants to die? Who wants to commit suicide just to... just to... just to... make an ENTIRE WORLD FREE FOREVER? Free from wars, militaries, governments, taxes, political oppression. Free from the kind of totalitarian governments that existed and currently exist. Free from the Holocausts that have killed Jews, Cambodians, Armenians, Russian Kulaks, Iraqi Kurds, Chinese dissidents, Native Americans, and oh so many others? "Who, exactly, would be stupid enough to risk death to make the world free???"

Everyone who volunteered to fight to fight Hitler, to name just one example. Remember, or have we forgotten so soon, that occasionally people die to keep the rest of us free. That's the way it's been for hundreds of years. The United States of America was founded by people who risked death to shake off the yoke of a government that was, by the standards of the day, not particularly bad.

Think about it. Somebody had to be the first one to start banging on the Berlin Wall, with a sledgehammer, in 1989. Somebody had to be the first to walk through. Somebody had to be the first to stand up and say, "Enough!" And the ironic thing is, the most strangely unusual thing, is that the entire Eastern Bloc fell, almost bloodlessly, in a couple weeks, because one by one everybody realized that all that's sometimes required is to finally stand up and be counted, and to just say no to the government. When the time was right, all it took was a slight push and the dominoes tumbled down.

Now, don't get me wrong. I'm not suggesting that EVERYONE would be identified. The "donors" to the system would remain perfectly anonymous, and the "guessers" would likewise be perfectly anonymous, but the organization itself would be made up of real people, who have published addresses, who have simply decided that they have had enough of the current system and are going to participate in a PERFECTLY LEGAL enterprise by the laws of the country, and just DARE the government to try to stop them. The organization wouldn't have to buy ads; the publicity firestorm would be enormous. Suddenly, all the politicians would be put on the spot! Instead of being asked by the reporters for their position on the economy, pollution, the budget deficit, or some other thing, they'll ask, "Why should the public NOT want to see you dead?"

When would be the best time to do it? Why, during a major political campaign! When Congress is out of session, and they can't pass legislation without calling some sort of emergency session. But it won't matter anyway, for a few weeks the organization doesn't actually have to take bets or make payments, they'll merely publicize their efforts for all to see. To reassure the public, they could announce that they'll only take bets on elected and appointed political officeholders...and anyone who tries to stop the system. And the politicians will be scurrying around, looking for political cover, trying to figure out how to NOT look scared, but at the same time each is wondering if he'll be the first to go. And all the while, the public will be loving it, laughing at the efforts of the politicos to cover their collective asses, and taking private bets among themselves on who will be the first one to die.

Prosecute the participants? On what charge? "Conspiracy to commit gambling"? Which prosecutor would risk appearing to be impeding the progress of a useful system? At that point, the organization's members will just be publicly exercising their first-amendment rights. Which judge would take the case? Now THEY'RE on the spot, THEY have to decide what to do. I contend that in an election year, before the election, there would be mass resignations from Congress, or members deciding "it's just not fun anymore" and decline to return even if re-elected, as well as the complete loss of whatever residual confidence the public has in the government. Whew! Is this all just wishful thinking? I really don't know!

[End]

Welcome to Wired News. Skip directly to: Search Box, Section Navigation, Content.

WIRED NEWS

Search:

News | | Search

Text Size: A A A A Home Business Culture Technology Politics Wired Mag Animation

'Cyber-Terrorist' Jailed Again

By Declan McCullagh

Story location: http://www.wired.com/news/politics/0,1283,40300,00.html

02:00 AM Nov. 21, 2000 PT

Jim Bell is nothing if not determined.

Just seven months after being released from prison, the 42-year-old convicted felon whom the U.S. government once dubbed a techno-terrorist is back in jail, this time for allegedly trying to intimidate IRS agents.

Bell was arrested last Friday, a week after the IRS and U.S. Marshals raided the home he shares with his parents in Vancouver, Washington. He has been charged with two counts of violating federal stalking laws.

Bell was arraigned Monday before Magistrate Judge J. Kelly Arnold in Tacoma, Washington and is being held without bail at the Federal Detention Center near Seattle.

In a series of telephone interviews in the days leading up to his arrest, Bell claimed he was compiling evidence of a government conspiracy to conduct illegal surveillance against him and unlawfully bug his home. "One guess is that I was getting a little too close to these people," Bell said.

Bell, a cypherpunk who pleaded guilty in July 1997 to interfering with IRS agents and using false Social Security numbers, is best known for a scheme he popularized that would use encryption, anonymity and digital cash to bring about the annihilation of all forms of government. He even gave it a catchy title: "Assassination Politics."

When the feds searched Bell's home earlier this month, according to a one-page attachment to the search warrant, agents were looking for "items which refer to Assassination Politics." They also hoped to find items that "contain the names, home addresses, or other information relating to current or past BATF, IRS, or other government or law enforcement employees."

Bell says that he's put his Assassination Politics proposal on hold. But he acknowledges that he showed up at the homes of suspected BATF agents and has done DMV searches on their names -- all in an effort to let them know that surveillance can be done in both directions.

"The double standard here is simply incredible," Bell said. "They simply don't like the idea that Jim Bell can simply look through a few databases, find one of their people, and publish the name on the Internet. They hate that."

"They're trying to make it look like I've been intimidating them. They've been intimidating me," Bell said. "I wasn't all that happy before, but I'm hopping mad ... if you think this is going to stop me, baloney."

Bell also said that he believed the Feds had illegally installed a tracking device in his car that would receive GPS signals and transmit the vehicle's location. He said he had contacted a security firm and asked them to locate it.

His attorney, Robert Leen of Seattle, said Bell's next court hearing is scheduled at 3:30 pm for November 22 before Judge Arnold and that the government is asking that he be held without bail.

"Mr. Bell's preliminary hearing is scheduled for the week of November 27, 2000. At that time Judge Arnold will determine whether there is probable cause to believe that Mr. Bell committed the crimes charged in the criminal complaint," Leen said in an email message to Wired News.

The 16-page complaint sworn by Philip Scott, an agent for the Treasury Department's Inspector General for Tax Administration, says Bell was a former "member of a militia organization" and had crossed state lines to track down information about federal agents including one named Jeff Gordon who had participated in previous prosecutions of Bell.

The complaint says that when agents raided Bell's home, they found notes on a women named Barbara Gordon who was married to a man named Jeff Gordon, with a son named Joshua. "Jeff and Barbara Gordon of Tualatin are not related to Special Agent Gordon," the complaint says.

Bell has been charged with violating 18 USC 2281, which prohibits some forms of stalking and intimidating the family of a federal agent.

"Jim had said he was going out ... about 8:30 Friday night. When he didn't come back around 10 p.m. they got a call from the police saying he had been arrested for stalking," said Milo Wadlin, Bell's brother-in-law who lives in Portland, Oregon.

U.S. News and World Report featured Bell as part of a cover story on terrorism. The story said that when agents raided his home, they found "volatile solvents, explosives ingredients, sodium cyanide, nitric acid, and disopropyl fluorophosphate -- one of several ingredients that, if properly mixed, form nerve gas -- all in a residential neighborhood."

Welcome to Wired News. Skip directly to: Search Box, Section Navigation, Content.

WIRED NEWS

Search:

News [ ] Search

Text Size: A A A A Home Business Culture Technology Politics Wired Mag Animation

IRS Raids Cypherpunk's House

By Declan McCullagh

Story location: http://www.wired.com/news/politics/0,1283,40102,00.html

02:00 AM Nov. 11, 2000 PT

WASHINGTON -- When a dozen armed federal agents invaded Jim Bell's home this week, he wasn't exactly surprised.

Ever since Bell, a cypherpunk whom the U.S. government has dubbed a techno-terrorist, was released from prison in April, he's predicted another confrontation with the Feds.

"They're basically trying to harass me," Bell said in a telephone interview. He has not been arrested or charged with a crime.

In 1996, Bell attracted the unwelcome attention of the IRS and the U.S. Secret Service after they learned he was talking up a plan to promote the assassination of miscreant bureaucrats through an unholy mix of encryption, anonymity and digital cash. Bell even gave his scheme a catchy title: "Assassination Politics."

Four years, three arrests and one plea-bargain later, Bell was released from the medium-security federal penitentiary in Phoenix, Arizona. Since then, he's been busy trying to prove allegations of illegal surveillance on the part of the Feds, including his charge that they unlawfully bugged his home.

For Bell, that meant spending the last six months compiling personal information about IRS and Bureau of Alcohol, Tobacco, and Firearms agents, a move that appears to have led to the six-hour search of his home in Vancouver, Washington.

Government offices were closed on Friday, and representatives were unavailable for comment. But the agents' search warrant cites "evidence of violations" of a federal law that prohibits intimidation of IRS agents.

The law says whoever "endeavors to intimidate or impede any officer or employee of the United States acting in an official capacity under this title" shall be fined up to $5,000 and imprisoned for up to three years.

A one-page attachment to the search warrant says agents were looking for items that "contain the names, home addresses, or other information relating to current or past BATF, IRS, or other government or law enforcement employees" and "items which refer to Assassination Politics."

Bell says that he's put his Assassination Politics proposal on hold. But he acknowledges that he's shown up at the homes of suspected BATF agents and has done DMV searches on their names -- all in an effort to let them know that surveillance can be done in both directions.

"I am thinking very strongly of picketing (IRS Agent) Jeff Gordon's house. I don't intend to violate any laws when I do that. It's conceivable that they won't appreciate my picketing their house," Bell says.

"I wasn't all that happy before, but I'm hopping mad.... If you think this is going to stop me, baloney," he says. "Needless to say I'm feeling very hostile. But I don't intend to violate black-letter Oregon law."

In Bell's 1997, plea agreement, he admitted to owning chemicals that could be used to produce Sarin gas and to stink-bombing the carpet outside an IRS office.

ElectionScramble.com: Political activists are scrambling to register election-themed domain names.

Indecision2000.org and indecision2000.net were snatched up early this week. At algorelost.org, George W. Bush loyalists are asking their allies to "certify the Bush victory" by signing an online petition.

PerpetualElection.com features frequently-updated news and commentary from liberals, conservatives, libertarians and greens.

The democrats.com folk launched trustthepeople.com to compile pro-Al Gore affidavits.

It's civics time: If you want to know how the presidential election might proceed, you might want to reread the U.S. Constitution.

The 12th Amendment outlines what happens if Florida's 25 electoral votes are still in dispute by the end of next month. The most likely scenario in such a case is that Al Gore would have a majority of votes cast and thus win the presidency.

But if Gore doesn't have a majority -- perhaps because of defecting electors causing a tie, which the outcome in Oregon could make more or less likely -- then the new members of the U.S. House of Representatives get to choose.

The catch is that there are only 50 votes: the "House of Representatives shall choose immediately, by ballot, the President, the votes shall be taken by states, the representation from each state having one vote." (As a side note, that means that residents of the District of

Columbia, which does not have a vote in the House, would not be represented.)

If the state delegations can't agree on Bush or Gore -- if, for instance, they have equal numbers of Democrats and Republicans in Congress, as Maryland does -- they wouldn't have a vote.

A preliminary Wired News analysis of the delegations suggests good news for Bush. He'd likely receive 26 votes from those red-on-TV states with Republican-majority delegations, while Gore would win 18. The rest would deadlock.

Achieving Electronic Privacy

A cryptographic invention known as a blind signature permits numbers to serve as electronic cash or to replace conventional identification. The author hopes it may return control of personal information to the individual.

by David Chaum, david@digicash.nl

This article appeared in Scientific American, August 1992, p. 96-101. Copyright (c) 1992 by Scientific American, Inc.

Every time you make a telephone call, purchase goods using a credit card, subscribe to a magazine or pay your taxes, that information goes into a data base somewhere. Furthermore, all these records can be linked so that they constitute in effect a single dossier on your life not only your medical and financial history but also what you buy, where you travel and whom you communicate with. It is almost impossible to learn the full extent of the files that various organizations keep on you, much less to assure their accuracy or to control who may gain access to them.

Organizations link records from different sources for their own protection. Certainly it is in the interest of a bank looking at a loan application to know that John Doe has defaulted on four similar loans in the past two years. The bank's possession of that information also helps its other customers, to whom the bank passes on the cost of bad loans. In addition, these records permit Jane Roe, whose payment history is impeccable, to establish a charge account at a shop that has never seen her before.

That same information in the wrong hands, however, provides neither protection for businesses nor better service for consumers. Thieves routinely use a stolen credit card number to trade on their victims' good payment records; murderers have tracked down their targets by consulting government-maintained address records. On another level, the U.S. Internal Revenue Service has attempted to single out taxpayers for audits based on estimates of household income compiled by mailing-list companies.

The growing amounts of information that different organizations collect about a person can be linked because all of them use the same key in the U.S. the social security number to identify the individual in question. This identifier-based approach perforce trades off security against individual liberties. The more information that organizations have (whether the intent is to protect them from fraud or simply to target marketing efforts), the less privacy and control people retain.

Over the past eight years, my colleagues and I at CWI (the Dutch nationally funded Center for Mathematics and Computer Science in Amsterdam) have developed a new approach, based on fundamental theoretical and practical advances in cryptography, that makes this trade-off unnecessary. Transactions employing these techniques avoid the possibility of fraud while maintaining the privacy of those who use them.

In our system, people would in effect give a different (but definitively verifiable) pseudonym to every organization they do business with and so make dossiers impossible. They could pay for goods in untraceable electronic cash or present digital credentials that serve the function of a banking passbook, driver's license or voter registration card without revealing their identity. At the same time, organizations would benefit from increased security and lower record-keeping costs.

Recent innovations in microelectronics make this vision practical by providing personal "representatives" that store and manage their owners' pseudonyms, credentials and cash. Microprocessors capable of carrying out the necessary algorithms have already been embedded in pocket computers the size and thickness of a credit card. Such systems have been tested on a small scale and could be in widespread use by the middle of this decade.

The starting point for this approach is the digital signature, first proposed in 1976 by Whitfield Diffie, then at Stanford University. A digital signature transforms the message that is signed so that anyone who reads it can be sure of who sent it [see "The Mathematics of Public-Key Cryptography", by Martin E. Hellman; Scientific American, August 1979]. These signatures employ a secret key used to sign messages and a public one used to verify them. Only a message signed with the private key can be verified by means of the public one. Thus, if Alice wants to send a signed message to Bob (these two are the cryptographic community's favorite hypothetical characters), she transforms it using her private key, and he applies her public key to make sure that it was she who sent it. The best methods known for producing forged signatures would require many years, even using computers billions of times faster than those now available.

To see how digital signatures can provide all manner of unforgeable credentials and other services, consider how they might be used to provide an electronic replacement for cash. The First Digital Bank would offer electronic bank notes: messages signed using a particular private key. All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key, which the bank has made a matter of record. First Digital would also make public a key to authenticate electronic documents sent from the bank to its customers.

To withdraw a dollar from the bank, Alice generates a note number (each note bears a different number, akin to the serial number on a bill); she chooses a 100-digit number at random so that the chance anyone else would generate the same one is negligible. She signs the number with the private key corresponding to her "digital pseudonym" (the public key that she has previously established for use with her account). The bank verifies Alice's signature and removes it from the note number, signs the note number with its worth-one-dollar signature and debits her account. It then returns the signed note along with a digitally signed withdrawal receipt for Alice's records. In practice, the creation, signing and transfer of note numbers would be carried out by Alice's card computer. The power of the cryptographic protocols, however, lies in the fact that they are secure regardless of physical medium: the same transactions could be carried out using only pencil and paper.

When Alice wants to pay for a purchase at Bob's shop, she connects her "smart" card with his card reader and transfers one of the signed note numbers the bank has given her. After verifying the bank's digital signature, Bob transmits the note to the bank, much as a merchant verifies a credit card transaction today. The bank reverifies its signature, checks the note against a list of those already spent and credits Bob's account. It then transmits a "deposit slip," once again unforgeably signed with the appropriate key. Bob hands the merchandise to Alice along with his own digitally signed receipt, completing the transaction.

This system provides security for all three parties. The signatures at each stage prevent any one from cheating either of the others: the shop cannot deny that it received payment, the bank cannot deny that it issued the notes or that it accepted them from the shop for deposit, and the customer can neither deny withdrawing the notes from her account nor spend them twice.

This system is secure, but it has no privacy. If the bank keeps track of note numbers, it can link each shop's deposit to the corresponding withdrawal and so determine precisely where and when Alice (or any other account holder) spends her money. The resulting dossier is far more intrusive than those now being compiled. Furthermore, records based on digital signatures are more vulnerable to abuse than conventional files. Not only are they self-authenticating (even if they are copied, the information they contain can be verified by anyone), but they also permit a person who has a particular kind of information to prove its existence without either giving the information away or revealing its source. For example, someone might be able to prove incontrovertibly that Bob had telephoned Alice on 12 separate occasions without having to reveal the time and place of any of the calls.

I have developed an extension of digital signatures, called blind signatures, that can restore privacy. Before sending a note number to the bank for signing, Alice in essence multiplies it by a random factor. Consequently, the bank knows nothing about what it is signing except that it carries Alice's digital signature. After receiving the blinded note signed by the bank, Alice divides out the blinding factor and uses the note as before.

The blinded note numbers are "unconditionally untraceable" that is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking the note numbers that Bob deposits with Alice's withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of Alice's random numbers. If she wishes, however, Alice can reveal these numbers and permit the notes to be stopped or traced.

Blinded electronic bank notes protect an individual's privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent. Such a verification procedure might be acceptable when large amounts of money are at stake, but it is far too expensive to use when someone is just buying a newspaper. To solve this problem, my colleagues Amos Fiat and Moni Naor and I have proposed a method for generating blinded notes that requires the payer to answer a random numeric query about each note when making a payment. Spending such a note once does not compromise unconditional untraceability, but spending it twice reveals enough information to make the payer's account easily traceable. In fact, it can yield a digitally signed confession that cannot be forged even by the bank.

Cards capable of such anonymous payments already exist. Indeed, DigiCash, a company with which I am associated, has installed equipment in two office buildings in Amsterdam that permits copiers, fax machines, cafeteria cash registers and even coffee vending machines to accept digital "bank notes." We have also demonstrated a system for automatic toll collection in which automobiles carry a card that responds to radioed requests for payment even as they are travelling at highway speeds.

My colleagues and I call a computer that handles such cryptographic transactions a "representative." A person might use different computers as representatives depending on which was convenient: Bob might purchase software (transmitted to him over a network) by using his home computer to produce the requisite digital signatures, go shopping with a "palm-top" personal computer and carry a smart credit card to the beach to pay for a drink or crab cakes. Any of these machines could represent Bob in a transaction as long as the digital signatures each generates are under his control.

Indeed, such computers can act as representatives for their owners in virtually any kind of transaction. Bob can trust his representative and Alice hers because they have each chosen their own machine and can reprogram it at will (or, in principle, build it from scratch). Organizations are protected by the cryptographic protocol and so do not have to trust the representatives.

The prototypical representative is a smart credit-card-size computer containing memory and a microprocessor. It also incorporates its own keypad and display so that its owner can control the data that are stored and exchanged. If a shop provided the keypad and display, it could intercept passwords on their way to the card or show one price to the customer and another to the card. Ideally, the card would communicate with terminals in banks and shops by a short-range communications link such as an infrared transceiver and so need never leave its owner's hands.

When asked to make a payment, the representative would present a summary of the particulars and await approval before releasing funds. It would also insist on electronic receipts from organizations at each stage of all transactions to substantiate its owner's position in case of dispute. By requiring a password akin to the PIN (personal identifying number) now used for bank cards, the representative could safeguard itself from abuse by thieves. Indeed, most people would probably keep backup copies of their keys, electronic bank notes and other data; they could recover their funds if a representative were lost or stolen.

Personal representatives offer excellent protection for individual privacy, but organizations might prefer a mechanism to protect their interests as strongly as possible. For example, a bank might want to prevent double spending of bank notes altogether rather than simply detecting it after the fact. Some organizations might also want to ensure that certain digital signatures are not copied and widely disseminated (even though the copying could be detected afterwards).

Organizations have already begun issuing tamperproof cards (in effect, their own representatives) programmed to prevent undesirable behavior. But these cards can act as "Little Brothers" in everyone's pocket.

We have developed a system that satisfies both sides. An observer a tamper-resistant computer chip, issued by some entity that organizations can trust acts like a notary and certifies the behavior of a representative in which it is embedded. Philips Industries has recently introduced a tamperresistant chip that has enough computing power to generate and verify digital signatures. Since then, Siemens, Thomson CSF and Motorola have announced plans for similar circuits, any of which could easily serve as an observer.

The central idea behind the protocol for observers is that the observer does not trust the representative in which it resides, nor does the representative trust the observer. Indeed, the representative must be able to control all data passing to or from the observer; otherwise the tamperproof chip might be able to leak information to the world at large.

When Alice first acquires an observer, she places it in her smart-card representative and takes it to a validating authority. The observer generates a batch of public and private key pairs from a combination of its own random numbers and numbers supplied by the card. The observer does not reveal its numbers but reveals enough information about them so that the card can later check whether its numbers were in fact used to produce the resulting keys. The card also produces random data that the observer will use to blind each key.

Then the observer blinds the public keys, signs them with a special built-in key and gives them to the card. The card verifies the blinding and the signature and checks the keys to make sure they were correctly generated. It passes the blinded, signed keys to the validating authority, which recognizes the observer's built-in signature, removes it and signs the blinded keys with its own key. The authority passes the keys back to the card, which unblinds them. These keys, bearing the signature of the validating authority, serve as digital pseudonyms for future transactions; Alice can draw on them as needed.

An observer could easily prevent (rather than merely detect) double spending of electronic bank notes. When Alice withdraws money from her bank, the observer witnesses the process and so knows what notes she received. At Bob's shop, when Alice hands over a note from the bank, she also hands over a digital pseudonym (which she need use only once) signed by the validating authority. Then the observer, using the secret key corresponding to the validated pseudonym, signs a statement certifying that the note will be spent only once, at Bob's shop and at this particular time and date. Alice's card verifies the signed statement to make sure that the observer does not leak any information and passes it to Bob. The observer is programmed to sign only one such statement for any given note.

Many transactions do not simply require a transfer of money. Instead they involve credentials information about an individual's relationship to some organization. In today's identifier-based world, all of a person's credentials are easily linked. If Alice is deciding whether to sell Bob insurance, for example, she can use his name and date of birth to gain access to his credit status, medical records, motor vehicle file and criminal record, if any.

Using a representative, however, Bob would establish relationships with different organizations under different digital pseudonyms. Each of them can recognize him unambiguously, but none of their records can be linked.

In order to be of use, a digital credential must serve the same function as a paper-based credential such as a driver's license or a credit report. It must convince someone that the person attached to it stands in a particular relation to some issuing authority. The name, photograph, address, physical description and code number on a driver's license, for example, serve merely to link it to a particular person and to the corresponding record in a data base. Just as a bank can issue unforgeable, untraceable electronic cash, so too could a university issue signed digital diplomas or a credit-reporting bureau issue signatures indicating a person's ability to repay a loan.

When the young Bob graduates with honors in medieval literature, for example, the university registrar gives his representative a digitally signed message asserting his academic credentials. When Bob applies to graduate school, however, he does not show the admissions committee that message. Instead his representative asks its observer to sign a statement that he has a B.A. cum laude and that he qualifies for financial aid based on at least one of the university's criteria (but without revealing which ones). The observer, which has verified and stored each of Bob's credentials as they come in, simply checks its memory and signs the statement if it is true.

In addition to answering just the right question and being more reliable than paper ones, digital credentials would be both easier for individuals to obtain and to show and cheaper for organizations to issue and to authenticate. People would no longer need to fill out long and revealing forms. Instead their representatives would convince organizations that they meet particular requirements without disclosing any more than the simple fact of qualification. Because such credentials reveal no unnecessary information, people would be willing to use them even in contexts where they would not willingly show identification, thus enhancing security and giving the organization more useful data than it would otherwise acquire.

Positive credentials, however, are not the only kind that people acquire. They may also acquire negative credentials, which they would prefer to conceal: felony convictions, license suspensions or statements of pending bankruptcy. In many cases, individuals will give organizations the right to inflict negative credentials on them in return for some service. For instance, when Alice borrows books from a library, her observer would be instructed to register an overdue notice unless it had received a receipt for the books' return within some fixed time.

Once the observer has registered a negative credential, an organization can find out about it simply by asking the observer (through the representative) to sign a message attesting to its presence or absence. Although a representative could muzzle the observer, it could not forge an assertion about the state of its credentials. In other cases, organizations might simply take the lack of a positive credential as a negative one. If Bob signs up for skydiving lessons, his instructors may assume that he is medically unfit unless they see a credential to the contrary.

For most credentials, the digital signature of an observer is sufficient to convince anyone of its authenticity. Under some circumstances, however, an organization might insist that an observer demonstrate its physical presence. Otherwise, for example, any number of people might be able to gain access to nontransferable credentials (perhaps a health club membership) by using representatives connected by concealed communications links to another representative containing the desired credential.

Moreover, the observer must carry out this persuasion while its input and output are under the control of the representative that contains it. When Alice arrives at her gym, the card reader at the door sends her observer a series of single-bit challenges. The observer immediately responds to each challenge with a random bit that is encoded by the card on its way back to the organization. The speed of the observer's response establishes that it is inside the card (since processing a single bit introduces almost no delay compared with the time that signals take to traverse a wire). After a few dozen iterations the card reveals to the observer how it encoded the responses; the observer signs a statement including the challenges and encoded responses only if it has been a party to that challengeresponse sequence. This process convinces the organization of the observer's presence without allowing the observer to leak information.

Organizations can also issue credentials using methods that depend on cryptography alone rather than on observers. Although currently practical approaches can handle only relatively simple queries, Gilles Brassard of the University of Montreal, Claude Cripeau of the Icole Normale Supirieure and I have shown how to answer arbitrary combinations of questions about even the most complex credentials while maintaining unconditional unlinkability. The concealment of purely cryptographic negative credentials could be detected by the same kinds of techniques that detect double spending of electronic bank notes. And a combination of these cryptographic methods with observers would offer accountability after the fact even if the observer chip were somehow compromised.

The improved security and privacy of digital pseudonyms exact a price: responsibility. At present, for example, people can disavow credit card purchases made over the telephone or cash withdrawals from an automatic teller machine (ATM). The burden of proof is on the bank to show that no one else could have made the purchase or withdrawal. If computerized representatives become widespread, owners will establish all their own passwords and so control access to their representatives. They will be unable to disavow a representative's actions.

Current tamper-resistant systems such as ATMs and their associated cards typically rely on weak, inflexible security procedures because they must be used by people who are neither highly competent nor overly concerned about security. If people supply their own representatives, they can program them for varying levels of security as they see fit. (Those who wish to trust their assets to a single four-digit code are free to do so, of course.) Bob might use a short PIN (or none at all) to authorize minor transactions and a longer password for major ones. To protect himself from a robber who might force him to give up his passwords at gunpoint, he could use a "duress code" that would cause the card to appear to operate normally while hiding its more important assets or credentials or perhaps alerting the authorities that it had been stolen.

A personal representative could also recognize its owner by methods that most people would consider unreasonably intrusive in an identifier-based system; a notebook computer, for example, might verify its owner's voice or even fingerprints. A supermarket checkout scanner capable of recognizing a person's thumbprint and debiting the cost of groceries from their savings account is Orwellian at best. In contrast, a smart credit card that knows its owner's touch and doles out electronic bank notes is both anonymous and safer than cash. In addition, incorporating some essential part of such identification technology into the tamperproof observer would make such a card suitable even for very high security applications.

Computerized transactions of all kinds are becoming ever more pervasive. More than half a dozen countries have developed or are testing chip cards that would replace cash. In Denmark, a consortium of banking, utility and transport companies has announced a card that would replace coins and small bills; in France, the telecommunications authorities have proposed general use of the smart cards now used at pay telephones. The government of Singapore has requested bids for a system that would communicate with cars and charge their smart cards as they pass various points on a road (as opposed to the simple vehicle identification systems already in use in the U.S. and elsewhere). And cable and satellite broadcasters are experimenting with smart cards for delivering pay-per-view television. All these systems, however, are based on cards that identify themselves during every transaction.

If the trend toward identifier-based smart cards continues, personal privacy will be increasingly eroded. But in this conflict between organizational security and individual liberty, neither side emerges as a clear winner. Each round of improved identification techniques, sophisticated data analysis or extended linking can be frustrated by widespread noncompliance or even legislated limits, which in turn may engender attempts at further control.

Meanwhile, in a system based on representatives and observers, organizations stand to gain competitive and political advantages from increased public confidence (in addition to the lower costs of pseudonymous record-keeping). And individuals, by maintaining their own cryptographically guaranteed records and making only necessary disclosures, will be able to protect their privacy without infringing on the legitimate needs of those with whom they do business.

The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. In one direction lies unprecedented scrutiny and control of people's lives, in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates.

Further Reading:

- Security Without Identification: Transaction Systems to Make Big Brother Obsolete. David Chaum in Communications of the ACM, Vol. 28, No. 10, pages 1030-1044; October 1985.
- The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. David Chaum in Journal of Cryptology, Vol. 1, No. 1, pages 65-75; 1988.

- Modern Cryptology: A Tutorial. Gilles Brassard in
- Lecture Notes in Computer Science, Vol. 325. Springer-Verlag, 1988.
- Privacy Protected Payments: Unconditional Payer and/or Payee Untraceability. David Chaum in Smart Card 2000: The Future of IC Cards. Edited by David Chaum and Ingrid Schaumueller-Bichl. North-Holland, 1989.