Untraceable Payments, Extortion, and Other Bad Things

By Tim May
W.A.S.T.E.: Corralitos, CA
Email: tcmay@got.net

I've noticed a few references in the press, and maybe on this list, to the idea that because some bad things may be done with untraceable payments (true Chaumian digicash, not the watered down version offering only one-sided untraceability), that governments will "not allow" such untraceable payments.

This won't work. So long as there is at least *one* such service, anywhere in the world....

I'll explain.

A few definitions:

"Bad things" are the uses to which strong crypto, anonymous systems, information markets, untraceable payments, etc., may be put to commit various crimes and dastardly acts. For example, untraceable payments for untraceable contract assassinations (thus removing the primary means by which such contractors are caught, the arrangements to begin with and the payments). Or, espionage in which the spy transfers information digitally via a "digital dead drop," eliminating the need for a physical contact point (an obvious vulnerability, as recent cases have shown) and also allowing efficient payment via untraceable funds transfers. And extortion.

Extortion is an interesting example to focus on. "Pay $25,000 or the following action will occur." A bomb, a virus, release of secrets, etc. Blackmail is of course a form of extortion, as is kidnapping. The acts involving *physical* actions will of course be less affected by crypto advances than will purely information-domain acts, e.g., where secrets will be released unless a payment is made. Physical acts have a nexus of detection at the act itself, the kidnapping, the bomb-planting, etc. (Though often the original act is very hard to protect against, and traditionally it has been the payoff that has been the nexus for catching the perpetrator...with untraceable payments, kidnapping becomes less dangerous for the kidnapper, especially if he kills his victim...I surmise that new technology, such as cameras and wireless Net video calls will be used increasingly to provide the payer of a ransom increased assurance that the victim was still alive at the time the transfer was made...the video call could even go through remailers, if the frame rate was drastically reduced or if PipeNet comes into existence.)

But I'll focus on simple extortion, with no complications of physical, meatspace actions. Pure cyberspace.

"Untraceable payments" refer to payer- and payee-untraceable Chaum-style cash. Although for the discussions here of extortion, payee-untraceable (the person being paid would not be traceable is my sense of this term) digital cash would be sufficient; that the payment originated from XYZ Corporation or some account at the Bank of Albania would not stop the acts.

Chaum has in recent years attempted (I have to presume) to take the "edge" of fully-intraceable digital cash by making it only partly untraceable. Many of us hypothesized that "mixes" (as in remailers) could be used to fully-untraceabalize (?) even partly-traceable systems. I recall Lucky Green, Hal Finney, and others in such discussions. "Banks" were proposed to do this. Recently, Ian Goldberg claims to have a system which formally accomplishes this.

(Keep in mind my original claim, that all it takes is _one_ such system...)

Now suppose that the U.S. Government formally and officially and with actual enforcement halts all such untraceable

systems, at least in terms of U.S. banks, credit unions, local moneychangers, etc. Even halts all partly-untraceable systems, to head off the Goldberg Gambit.

Does this stop extortion?

Suppose there exists a supplier of fully-untraceable (or payee-untraceable at least) cash *somewhere* in the world. It could be a physical bank, a la the Bank of Albania, or it could be an underground payment system, a la the Mafia, the Tongs, the Triads, whatever. A reputation-reliant system which says "Present us with the proper set of numbers and we will provide money to the bearer, or follow instructions, and so on." (I'm informally describing the process of "redeeming" a digital bearer instrument, converting the set of numbers into some other form of specie, or item of value, whatever. Maybe gold, maybe dollars, maybe an entry into an account somewhere. The "untraceability," via the blinding operation, means that the bearer is not linked to the transaction made earlier, so there is not risk at the bank or Triad. I'm also not distinguishing between offline and online clearing here...my feeling for a long time has been that online clearing has many advantages, but I suspect it does not work too well in the extortion case described here, until something like PipeNet can be used as part of the process.)

So, Ed the Extortionist tells Vic the Victim to please purchase $25,000 worth of Bank of Albania crypto-credits, by whatever means he has to (including, presumably, even flying to Albania, or using other funds transfer mechanisms, or perhaps even using crypto credits he had accumulated in other transactions.) Whatever, it is assumed that Vic _wants_ to make the transaction, just as with kidnap ransom demands. (Not "want" in the ultimate sense, but "want" in the sense of the local transaction. In extortion and kidnap cases, the victim of the extortion or the family of the kidnap victim may choose not to make the payment...I'm dealing with the more interesting case of where the payment is being made.)

How Ed receives the funds without the bits being followed through cyberspace is of course an easy exercise for readers here. Anonymous remailers with reply-block capabilities, a la Mixmaster, or, my preference, posting in a public place, a la the Usenet or other widely-disseminated message pools.

Ed takes the crypto credits and redeems them as he sees fit (after some unblinding stuff, of course). The redemption order is unlinkable to the extortion. (Modulo the usual issues: if Ed and Vic happened to be the _only_ users of such a system, then of course simple input-output mapping would finger Ed, as with such uses of remailer networks. Correlations are always a danger. Correlations in timing, in deposit size, etc. The usual fixes apply: more users, more bits sloshing around the network, time delays, etc. Offline clearing facillitates some of these measures. Ditto for breaking up the payment into N separate smaller-denomination transfers.)

What could the U.S. do? If Vic the Victim is careful, and either flies to Europe or the Caribbean to make the arrangements, or uses various Cypherpunks-type communication methods, he should be able to wire money from a conventional account, or use real cash, and purchase the crypto credits from the Bank of Albania. Likewise, if Ed the Extortionist has freedom of travel or freedom to use various channels, he can cash in his crypto credits. This no matter what the U.S. does.

So, even if "Mark Twain Bank" and "Bank of America," and, indeed, the rest of the U.S. banking establishment eschews untraceability, the presence of such services anywhere in the world is enough to make the act described workable. And that "anywhere in the world" can, as I mentioned earlier, encompass the various underground banking systems already widely in use (Tongs, Triads, chop marks, etc. in Asia, and presumably similar systems elsewhere). Or it could encompass fairly conventional banks which offer such untraceable routes for a premium. A $5,000 commission on top of the $25,000 transfer would make a lot of the world's banks sit up and take notice. And so long as they were not told what the fund transfer was all about--Vic is unlikely to gain anything by telling them--they have plausible deniability and moral comfort.

Yes, this has all been obvious for a while. (The mapping of the scenario I describe to a specific digital cash system depends of course on the nature of the system, on cryptographic protocols, and so forth.)

And I surmise that the U.S. Government must have realized this. And realized that only by _completely quashing_ all

such untraceable payments systems can the goals of stopping such "bad uses" be met.

Unfortunately for them, and unfortunately for the victims of such crimes, no such worldwide stoppage of all such systems seems possible, even with draconian police state measures. There are just too many interstices for the bits to hide. And too much economic incentive for some persons or banks to offer such funds transfer methods.

Fortunately for the bulk of us, the likely number of deaths and economic losses from such crimes of kidnapping, extortion, and even murder for hire, is still likely to be vastly lower than the number of deaths caused by powerful central governments enriching themselves and their cronies with foreign wars. Not to mention the deaths in the Drug War, the lives wasted in other interferences in private behavior, etc.

This is why I look forward to this Brave New World of fully untraceable communications and fully untraceable economic transactions.