4 law.co.il

For Law Enforcement Use Only

Brazil 9/04 Boaz Guttman Adv.

Breaking Digital Evidence in Court – Supplement 4

Digital Issue in Israeli Cyber Crime Case – 18/2/04 & 25/7/04

Background:

17/8/04

The wireless hacker – the secret service could`nt break the encryption

" The computer was encoded in such a complex way, that all the experts of the police and the General Security Agency tried and failed to break into Dudi's handheld computer, which was confiscated from his person.In view of that, the police was forced to turn to a private company that has expertise in this field, and which requested NIS 157,000 to break into that computer, informing us that the process would take 25 work-days…" Haifa District Attorney

Wireless Hacker Dudi Sternberg in Court

David Sternberg (Dudi), 27, apparently some species of hacker, decided to use his skills to make money in ways the prosecution claims are not entirely kosher.

He and another partner, Adi Aloni, were accused at the Haifa Magistrates Court that in 2003, they conspired to steal money by hacking into the Postal Bank computers. They did their deeds by making fictitious deposits into other people's accounts. These others were to have withdrawn the money thus deposited, and share it with the miscreants.

The Postal Bank in Haifa

Sternberg and Aloni bought wireless routers and modem cards, explain the prosecutors. In parallel they told a number of people to open accounts at the Postal Bank, for the deposits to be made.

Sternberg and Aloni bought wireless routers – one of the routers seized…

In November and December 2003, there were multiple break-ins to the Haifa Hod Hacarmel Postal Bank branch. Apparently that was when a wireless router was installed in the bank's communications closet.

That router, allege the prosecutors, enabled the hackers to hook up to the bank's computer system. They also claim that the defendants rented a desk at a mediation office next door to the bank, where Sternberg installed a computer system. And that is how Sternberg and Aloni managed to make the fictitious deposits in the accounts, NIS 237,000 in total, from which the customers withdrew NIS 125,000. 1$ = 4.5 NIS.

The charges include breaking into the bank's computer system, implanting a virus there, and embezzlement. While about it, the prosecutors also allege that the twosome tried to break into the Bank of Jerusalem website too. The prosecutors told the judge in the courtroom that the police as well as the Israeli secret service (called also Shin Bet or Shabak) failed to open the digital media which was encrypted. Therefore a private company was paid the total sum of 157,000 NIS – they told by an **expert opinion** to the prosecution that they broke Dudi`s encryption…Below the relevant court protocol deals with the Modus Operandi of the hacker as well as his lawyer claim and **Dudi`s claim:" The opinion says nothing…"**

The Haifa judge ordered they remain behind bars…

Haifa`s Magistrate Judge KAMAL KHAYR

Anyway, Sternberg and Aloni were arrested in January 2004, and a Haifa judge ordered they remain behind bars until the end of the hearings. Sternberg was in fact already incarcerated over another affair entirely, being heard at a Nazareth court.

Alony however appealed his incarceration until the end of proceedings. The District Court rejected his appeal, but the Supreme Court reversed it, remanding Alony to full house-arrest. Then Sternberg appealed too.

But the District Court did not accept his claim that he was being treated prejudicially, pointing out that he, not Alony, was the computer whiz. He is therefore a risk to the community in that he might carry out more computer crime, whereas Alony is not.

Sternberg also appealed to the Supreme Court. In the hearing before Justice Salim Joubran, the prosecutor said the FBI is also investigating the Israeli hacker, suspecting he broke into the computer systems of an American company.

Supreme Court. Justice Salim Joubran

Essentially, the prosecution's argument is that Sternberg is a genius. He's a master hacker who can break into remote sites and wreak havoc. The police found only one router, the prosecutor added: there are two more out there that Sternberg could use for nefarious purposes if released. They are like loaded guns, the prosecution wailed, just waiting to be used.

To which Sternberg's lawyers rebutted that the state hasn't provided irrefutable evidence that his client is as smart as that.As his Lawyer said in the first stage during the prosecution request:" I deny the facts linking the respondents to the committing of the offences, i.e., breaking into the bank. **Let them show us one piece of evidence that they broke in**. I deny that they gave instructions. **Let them show us that that actions was carried out in the computer**…"Quite the contrary, he's a dolt who failed to hack into the Bank of Jerusalem, and he couldn't even penetrate the Postal Bank computer

system from afar, like any self-respecting hacker would. He needed a router to do it, which he had physically installed by breaking into the bank like a common thief. Some genius.

Joubran wasn't impressed. He rejected the appeal and ruled that Sternberg is clearly a computer genius who poses a danger. Technically he has the capacity to commit crimes by pressing a button from his home. No two ways about it, Joubran ruled; genius or git, Sternberg must stay behind bars .The decision (the second in this court) in the Supreme Court was in **25/7/04**.Translation below.

It was not the first time a hacker was arrested in the Supreme Court till the end of his trial. In **7/9/99** first time ever in the Supreme Court Justice Dorit Banish ordered to hold in jail till the end of the trial one of the three blind hackers – The Badir brothers. The court said :`There is a danger in computer related crimes that requires imprisonment without bail`.This Magistrate court protocol presents the field in which the Defense Lawyer has to attack…Some slides in the PPT as well as the speech presents the issues – How to Break Digital Evidence in Court?.Needless to say from the other hand that the court ruled already in the Badir Case (2001) that:"…6.Circumctantial evidence plays a crucial role in proving the responsibility of a computer felon…12.There is no need to prove the computer expertise of the criminal…."Source: http://www.4law.co.il/badir.html

But the rule of the Defense Lawyer did not start in full effort yet….

THE COURTS

Haifa Magistrates Court		BS 001804/04	
		Principal: P 001516/04	
Before:	Justice Kamal KHayr	Date:	**18/02/2004**

In the matter of: **The State of Israel** Applicant(s)

Versus

1. **David Sternberg** Respondent(s)
2. **Eddie Alloni**

…

Attorney Rosenthal-Ne'eman:

Repeats the request.

In the matter of the prima facie evidence – following discrepancies that were found at the Postal Bank, refers to the exhibit marked 10.
An inquiry was launched at the Postal Bank on 5 January 2004; a foreign body - a wireless router – was discovered inside the communications console in the Postal Bank branch in the Danya neighborhood.
Refers to exhibits 6 and 7.
The respondents hired a desk at Immobilia, a real-estate agency which has a shared wall with the Danya branch of the Postal Bank.
The evidence file contains a receipt for weekly rent, made out in the name of Eddie Alloni, in the amount of NIS 450. It was found in the document file A and marked 200.
Evidence was given by Asher Cohen, the owner of the real-estate agency, on 15 January 2004. On page 1, line 12, it states that he ran an advertisement to rent the asset, Eddie phoned him, and Dudi (David) and Eddie came to Cohen's office.
I will ask the court not to adopt the version that Eddie allegedly did not know about Dudi's actions, since we have clear evidence of this – which I will present.
There is further evidence given by an employee at the real-estate agency, on page 1 line 8, describing how Eddie and Dudi came there to rent the table. Refers to p. 2, line 18.

Attorney Goldberg:
I deny the facts linking the respondents to the committing of the offences, i.e., breaking into the bank. Let them show us one piece of evidence that they broke in. I deny that they gave instructions. Let them show us that that actions was carried out in the computer.

Attorney Rosenthal-Ne'eman:
The computer was encoded in such a complex way, that all the experts of the police and the General Security Agency tried and failed to break into Dudi's handheld computer, which was confiscated from his person.
In view of that, the police was forced to turn to a private company that has expertise in this field, and which requested NIS 157,000 to break into that computer, informing us that the process would take 25 work-days. Obviously, the respondents did not remain in custody during that time. We filed an indictment that we have enough evidence connecting them to the offences. Today we received the evidence given by the person who managed to break

into the computer; he stated his opinion, which I wanted to present to my colleagues: it arrived with a police officer today.
There is a close relationship between the defendants; Dudi is 25 and Eddie is 54 and their relationship is rather unusual.
Refers to the evidence of Dudi's girlfriend, Sivan Shoshan, line 66, describing the relationship between the two, and so forth.
The blue file contains an entire communications research-study, which clearly shows the strong relationship between the two respondents, and between Respondent 1 and the people who withdrew the funds and opened the accounts in which the funds were deposited. There are numerous telephone-calls, incoming and outgoing.
Eddie Alloni was interrogated regarding those relationships but chose the right to silence. The two respondents both chose to remain silent. This further reinforces the evidence against them.
There are detailed testimonies in clause 3 of the indictment, in which each one gave a contradictory version.
They bought the router from a salesman – Moshe Ravid - who attested that on 10 August 2003, the respondents came to him, Eddie took out cash money and paid for the router. Note that the wireless router that was removed from the communications console in the Postal Bank branch was identified by Ravid as the same one that he had sold to the respondents. Moreover, the packaging that was confiscated in the respondent's house contained an invoice made out in the name of Dudi and a certain company that is non-existent.
In the handheld computer of Respondent 1, which was broken into, various hacker software programs were found. The laptop computer was also broken into and it was revealed that the username is Rabak - the same name used by the person who hacked into the postal bank computers.
Respondent 1 is accused of a second charge, that of attempting to break into the Bank of Jerusalem. Also found in the possession of Respondent 1 at the time of his arrest on 15 January were disks containing software programs for hacking into the Bank of Jerusalem. The disks were taken for examination and it was found that the log matched the log with which the break-in was attempted. There is conclusive evidence that the break-in was performed, including the exact hour and day. It is not possible that it is a question of another hacker.

I note that he was arrested on 15 January, when he was in the real-estate office and was seen by chance by detectives who came to reconstruct the wireless router. Apparently, he was unable to get rid of the disks.

We have evidence concerning the expertise of Respondent 1, and a great number of testimonies.

What can be elicited from the file is that Dudi was the technical man who hacked into computers, while Respondent 2 managed all the other matters, creating contacts with the people who opened accounts. He brought Dudi.

There is no doubt that there is prima facie evidence in this case, and not circumstantial evidence.

The same wireless router cannot transmit further than 100 meters. In other words, a place had to be found that was close to the communications console in the postal bank branch.

As for the grounds for arrest, it is well known and backed up by rulings as well, that there are also grounds for arrest in property offences. I present a ruling.

In the case before us, Eddie was a full partner. That is, even if he claims that he is not dangerous because he doesn't know how to operate a computer, he is a full partner, as shown from the evidentiary material – he created the infrastructure. He presents exactly the same danger.

Note that in our case, three routers were purchased – we still do not know where the other two are. The danger remains.

Moreover, Respondent 2 proved his dangerousness by committing the offences while serving a community service sentence. We ask that Respondent 2 not be considered a free man, since community service is imprisonment for all intents and purposes.

He received a "prize" and in fact he stands before us as a prisoner for all intents and purposes. If we were looking at a prisoner on leave who committed offences, the court would immediately instruct his detention until the end of procedures. This is how the matter should be regarded.

Refers to the verdict in this court a few months previously regarding Mr. Alloni for offences of bribery and fraud,

I refer to the arguments of the defense attorney who presented Alloni as a man who was exposed to a severe temptation just one time. The accused himself expressed deep regret for this and asked his situation to be taken into account.

Concerning Respondent no. 1, I present a criminal record, including an offence of fraud and extortion and he should remain in custody until the end of proceedings.

Presented and marked M/1.

In the matter of releasing Respondent no. 2 while in custody, we have a ruling in connection with a case resembling the case at bar, heard by Justice Cheshin. There is therefore room to arrest him.

Ahead of the hearing held in his matter, the court's decision is significant and the court must take this into account.

There are fears concerning the obstruction of justice if the respondents are released, because of the relationship between them and with the others involved.

The proceedings are dynamic and during the trial there may be a further obstruction.

There is immense danger in the case before us, since the method used is an innovative one. Nothing of this kind has been attempted before, and had their actions not been discovered in time, they could have caused the total collapse of the banks.

Presents the evidentiary material to the court.

Attorney Goldberg:

The indictment, on the face of it, according to its content and the evidence that my colleague noted, can in no way constitute even prima facie evidence, even circumstantial evidence, connecting the accused with the suspicions attributed to them. This takes into account the following facts; there is no evidence, as the court has seen, that the two respondents broke into the Postal Bank and placed anything there.

The prosecution says that a wireless router was installed there. That sort of router can be used only one or two kilometers from the site. The expert witness says - regarding the use of that router, in accordance with the conditions of the surroundings - at far greater distances. Let us take the 100 meters. In the Danya commercial center, there are numerous public areas and many buildings in the area. There is Beit Allon, a kindergarten in an area close by. What sort of idiot am I when it transpires that the only fact available is that I rented a table there?

This is a question of something planned in advance. They are accused of being sophisticated - geniuses in this field. Who would rent a place so close when there is 100 meters to work with? Obviously, if the police come and look

for burglars, they will go first to new arrivals in the area, and next to those nearby. It isn't reasonable that this would happen.

Alloni is doing community service as a result of what happened to him - his license as a driving teacher was revoked – and he was looking for something else to do. Dudi is known as an expert who develops all sorts of computer software programs and applications, including data security. Dudi told Eddie that he had lots of ideas and software and they could open a shop to sell computer software. Meanwhile, the owner of the agency said to them that the shop has an area of 270 meters and at the moment they were unable to rent it out. They were looking for an office to start marketing their goods and they rented a table there in the meantime. He worked there every day, doing research and applying his expertise in the sector, and would meet with people who came to test his ideas and buy them.

Because Eddie Alloni was doing community service, his input was negligible, and most of the work was done by Dudi.

They have a reasonable explanation for the place, backed up by a leasing contract. Matters are completely clear - they worked in daylight, openly. We will bring people who had business ties with them. The place was rented openly, and nothing underhand was involved.

The police say that the router's box was found – there are other boxes like these. Like any person who works with computers, he bought many kinds of equipment and among others, those as well. If I would want to use them to break into a computer, I would keep them close at hand, in my room.

There are many things that can be bought anywhere and that resemble each other like two peas in a pod. In this series, there were thousands of routers, and if some are found on my premises, does this link me to an offence?

Transcripts of phone-calls made by people with Eddie Alloni have been presented. I refer to their testimonies that they withdrew the money and have evidence. If their evidence mentions the respondents, then arrest them, but they all deny the respondents' connection with those invoices.

Those people are some of those who were his students when he was a driving teacher, they had relationships, and spoke on the phone. Each conversation can be explained.

Therefore, with all due respect, to rely on evidence of lists of phone-calls that can be explained, is not prima facie evidence.

In this absence of evidence, suddenly evidence is found that one respondent is aged 54 and the other is 25 – and that links them. Who has ever seen partners of such disparate ages?

For people who are partners in a specific business, age has no significance. This explains why they sought each other out. There is nothing surprising in their age difference, and it provides evidence of nothing at all.

It is beyond my powers to understand computers. I started to look for rulings on the questions of computers. I carried out an investigation to see whether it has ever happened in Israel that someone was arrested until the end of proceedings for computer-related offences. No one has ever been arrested. My colleague, in order to persuade the court, presented two rulings – one related to drugs and the other to fraud and extortion.

The prosecution and the police are not arguing the theft of secrets of Bank Leumi, but the great inherent danger in sophistication.

I wish to present a press-cutting of Attorney Guttman who is today a criminal lawyer, showing that there is no risk at all. There is no danger at all.

So we come to the duty imposed on the court by legislation and rulings - and if the court comes to the conclusion that there is any circumstantial evidence that can link them to the place, there is certainly no direct evidence.

Even then, that doesn't justify detention until the end of proceedings. There will be a trial, there are 70 witnesses, it could be a trial lasting some years - should they remain in custody?

Not only is there no room to arrest them because of the material and because no dangerous circumstances exist but also Alloni certainly has no idea about computers. It has been claimed that Alloni committed the offences while doing community service, then they say he did it in coordination with Sternberg.

In any case, if the court comes to the conclusion that there is room to detain them, it should and must seek any way, another option for this.

There is no doubt that, at the most, an alternative for arrest should be found. I do not see any room for continued arrest in the circumstances of the case. They attend every proceeding, they have fixed addresses. They have an office which will soon open in Danya, where they will start marketing computers and will succeed in the project they spoke about.

Therefore, in accordance with rulings, there is no reason to place them under lock and key, when an alternative exists, should the court come to the conclusion that there is a danger or that evidence exists.

We have received today an opinion - I haven't yet managed to speak with my clients - and I have studied it only briefly. On the face of it, the opinion was delivered to the police in order to link them with the theft. Nothing was determined. Only very general things were determined - that he uses the name Rabak…Maybe the hacker wanted to use his name of Rabak?

He indeed owns all sorts of hacker software, but this is the area of his work. In order to prevent break-ins, first of all one has to understand hacking. All the programs that prevent hacking are hacker software.
They say that they finally managed to hack into the computer, but the respondent said he was willing to open the computer, if they find a connection between the computer and the instruction given. Evidence for this must be submitted. He used hacker software programs in the framework of his work. Let them show evidence linking him to the instructions given to the Postal Bank.
They have nothing of the kind.

Respondent 1:

I have been involved in the field of data security for close to 10 years. I have to hack into computer systems in order to protect them, I receive authorization to do this. I received authorization from a credit company in Israel, from Bank Hapoalim, the Mizrahi Bank, and from government offices. This is what I do for a living. I develop this kind of software.
This field requires an understanding of all kinds of peripheral issues, such as communications. I have been involved in wireless communication for some 4 years. Had I wanted to hack into one bank or another, I had a hundred opportunities to do so. I never did it, and never will.
Regarding the opinion – the computer was confiscated on the fifteenth of the month, a month and three days ago. I said that I was willing to open the encoding, and that if nothing was found they should release me, but they said they couldn't release me.
I said I couldn't help them, and I don't want to, because I have no connection to the matter.
As soon as I saw they were trying to use force, I said that from here on, I've got nothing to say.
Some company - that according to the opinion say they are the only company that can reconstruct the computer - they have a security clearance and the appropriate skills to carry out reconstruction, as long as he had the computer, the person from this company said that this computer, two installations ago, had a user named Rabak. That doesn't mean a thing, I didn't have a confrontation with the people. This computer hasn't been plugged into electricity for eight months, and it's impossible to say when it was connected, and when files were installed in it. I have studied hacking in Israel and in Europe. I offered them all the tools. The opinion says nothing.

The Supreme Court

SCM 6864/04

Before: **The Honorable Justice Salim Joubran**
Applicant: **David Sternberg**

V.

Respondent: **The State of Israel**

Motion to appeal the judgment given on 21 May 2004 in the Haifa District Court, in CC 4096/04, by the Honorable Justice A. Raz

Date of the session: **25 July 2004**

For the Applicant: Attorney Allon Nesher; Attorney Sharon Ringer
For the Respondent: Attorney Dudu Zchariya

JUDGMENT

Before me is an appeal to overturn the ruling of the Haifa District Court (the Honorable Justice A. Raz), dated 21 May 2004, in case CC 4096/04, in which the ruling handed down by the Haifa Magistrates Court (the Honorable Justice K. Hir) of 29 April 2004, in case S.A. 1804/04, dismissing the petitioner's appeal to be released to an alternative form of detention, in his mother's home.

On 6 February 2004, an indictment – consisting of two charges - was served on the applicant and his partner, Eddie Alloni (hereinafter: "the Partner"). In the first charge, the following offences were attributed to both of them: conspiring to commit a crime; fraudulent information; computer trespass in order to commit another offence; a computer virus, and theft. The second

charge relates solely to the Applicant, attributing to him the offence of attempting to unlawfully access computer material.

According to the facts in the indictment, the Applicant conspired with the Partner for the two of them to carry out theft by connecting to the computers of the Postal Bank and by depositing fictitious money in the accounts of others, so that those others could thereafter withdraw the money. As part of the conspiracy and in order to advance it, the two purchased three wireless routers and a wireless modem card. They broke into the Hod Hacarmel Postal Bank branch in Haifa and installed one of the routers inside the communications console in the branch, enabling a wireless connection to the computer communications network of the Postal Bank. Some days later they rented space in an asset adjoining the postal bank branch, and installed computer equipment in that asset. Next, the Applicant, in coordination with the Partner, created wireless communication between his personal computer and the router that had been installed in the branch, and managed in this way to access the Postal Bank's computers. Moreover, the Applicant installed on the postal bank's computers various hacker software programs that would help him fraudulently deposit money in the customers accounts. The Applicant and his Partner instructed several people with whom they had conspired, to open accounts with the Postal Bank, with the intention of virtually depositing in them funds that would later be withdrawn in cash. Indeed, the Applicant effected deposits in those accounts, and the monies were withdrawn from the Postal Bank, following the instructions of the Applicant and his Partner.

The additional charge which relates to the Applicant alone, claims that on the date of his arrest (15 January 2004), various CDs were found in his possession, some of which contained hacker software. It is further claimed that a specific CD contained a software program enabling access - through security loopholes - to the Bank of Jerusalem's internet website, as well as a file documenting an attempt to hack into that website.

In tandem with the serving of the indictment, the State filed a request in the Haifa Magistrates Court for the arrest of the Applicant and his Partner until the end of legal proceedings against them.

On 18 February 2004, the Magistrates Court (the Honorable Justice K. Hir) instructed that the Applicant and his Partner remain under arrest until the end

of proceedings. It should be noted that the Applicant was already in custody until the end of proceedings conducted against him in another matter, that is being heard in the Magistrates Court of Nazareth.

The Partner's appeal against his detention until the end of legal proceedings against him, which was filed at the Haifa District Court (BS 3423/04) was dismissed on 29 February (the Honorable Justice Y. Cohen).

The Partner appealed this ruling in this court and on 7 March 2004, the Honorable Justice A. Gronis accepted the appeal and instructed that the Partner be released to full house-arrest.

On 15 April 2004, following the decision to release the Partner, the Applicant filed an appeal with the Haifa Magistrates Court to reconsider that judgment.

On 29 April 2004 the Magistrates Court dismissed the appeal, determining that the appeal to grant an alternative form of detention should not be allowed at this stage, for two reasons – first, since a distinction must be made between the Applicant and the Partner, and second the appeal was made too early – for the Applicant should have first obtained his release in the other case being conducted against him in the Nazareth Magistrates Court.

> The Applicant filed an appeal against this decision in the Haifa District Court.

On 21 May 2005, the District Court (the Honorable Justice A. Razi) dismissed the appeal because it is clear that the principle of equality and discrimination, where it concerns the issue of detention until the end of proceedings, is a great rule. And indeed in the first charge, the pivotal one, the same offences are attributed to both the Applicant and the Partner, but on the other hand, there is prima facie evidence showing that the Applicant, unlike the Partner, possesses know-how in the computer field. The significance of this is that only the Applicant poses the danger of more offences of this kind being committed. Therefore, the court ruled that it cannot be argued that distinguishing between him and his partner constitutes discrimination. Furthermore, the court noted that for the purpose of distinguishing between the two defendants, it is not enough that the Partner was released for several weeks and, moreover, because his early release resulted from an error made

by the State. A release granted, due to an error in discretion, to one defendant must not lead to the same mistake being applied to another defendant. The court added that the claim that enough time had elapsed and that court discussions were likely to be prolonged was not brought up in the magistrates court, and this matter should not be addressed at the present time when only a short period, relatively, has elapsed since the Applicant's arrest.

The appeal now before me was filed against that ruling.

The representatives of the Appellant claimed before me that, in terms of risk, there is no room to distinguish between the Appellant and his partner. They argued that the reason for the Partner's release by this court did not stem from his lack of knowledge in the computer field, and therefore the two must be judged equally: the ruling of this court concerning the Partner must be adopted for the present Applicant, too. In addition, they argued that the Applicant is a young man and that his criminal past in fraud is very old. The applicant's representatives further argue that because time has elapsed and the proceedings in the case are expected to be long - more than nine months - the Applicant must be released to an alternative form of detention.

Against this, the state's representative argues that a distinction must be drawn between the Applicant and his partner, because of the far greater risk posed by the Applicant. He argues that the Applicant has know-how and technical ability, which is explicitly demonstrated in the evidentiary material and in the conduct of the Applicant, shown in the file. He also maintains that the Applicant has a rich criminal record and is currently under investigation by the FBI for illegal access to the computers of an American company. The state's representative asserts that it is not possible to award the Applicant sufficient trust that could justify his release to an alternative form of detention.

After I studied the investigation case, and the judgments of the previous instances, and after having heard the arguments of the parties, I came to the conclusion that the appeal should be dismissed. I could find no flaw in the ruling of the district court.

My assumption is that prima facie evidence indeed exists and also that grounds for arrest also exist in the matter of the Applicant. The question that faced me is whether, in the circumstances described, it would be advisable to

consider an alternative form of detention for the Applicant. The answer to that question is negative.

The risk reflected by the Applicant is substantial. The Applicant is a computer "genius" who possesses the know-how and capacities enabling him to commit grave offences and cause huge damage. His professionalism is clearly reflected in the evidentiary material and also in his professional background. Unlike an offender of the "old-school", who - without physical access to his target – was unable to implement his schemes, the Applicant's technical abilities allow him to commit offences, with the click of a button, from his home. Therefore, it is not possible to achieve the goal of detention by releasing him to an alternative kind of detention.

Furthermore, the conclusions of the instances prior to this one are acceptable to me. There is no doubt as to the existence of prima facie evidence, attesting to the fact that - of the two partners in the offence - only the Applicant has know-how in the computer realm. The implication is that in everything connected to the charges we are dealing with, the risk of more offences of this kind being committed is posed chiefly by the Applicant, and therefore, there is no room to claim that distinguishing between the Applicant and the Partner constitutes discrimination. Even more so, let us not forget that the principle of equality and the prohibition of discrimination between defendants is not a supreme principle, that enjoys a prime position in every case: it must be balanced against other important considerations and its weight must be evaluated accordingly (see CC 5714/03 Yizhar Giovanni v. the State of Israel, AC 2003 (2) at 3416). Furthermore, in our matter, the Partner has already been released for some weeks. His release resulted from a discretionary error and should not lead to the same error being applied to other defendants.

On the basis of the aforegoing, I have decided to dismiss the appeal,

Given this day, **26 July 2004**