

**The Public Voice Civil Society Meeting:
"Next Generation Privacy Challenges and Opportunities"**

Jerusalem, Oct. 25, 2010

The Campaign Against the Biometric Database Act

Avner Pinchuk – The Association for Civil Rights in Israel

I wish to thank EPIC and the entire Public Voice coalition for the invitation. My name is Avner Pinchuk and I'm an attorney at ACRI - The Association for civil rights in Israel. ACRI is the leading human rights organization in Israel, which for the past 40 years has been working to defend and promote the entire spectrum of human rights in the country and in the occupied territories.

In 2009 we participated in a fierce public debate over the "Biometric Database Act". The legislation, which was enacted by the Knesset at the end of the year, empowers the Ministry of Interior to issue new ID cards and passports and to establish a biometric database, containing templates and images of fingerprint and facial scans of all Israeli residents. The alleged purpose of the biometric database was the need to prevent false pretense and ID card forgery. However, from the beginning there was a secondary use: the act enables the Israeli Police to receive information from the database under various circumstances.

All though the bill was passed nearly a year ago, the government has not began its implementation, and according to partial information we have obtained, there are serious disagreements within government ministries on the ways in which the Act will be implemented. I have reasons to assume, that the campaign against the bill has at least seeded some of the doubts and fears which are stalling the establishment of the database, and that efforts are made within the government to reduce the ramifications that the database will have on the protection of privacy and civil liberties.

ACRI campaigned against the "Biometric Database Act" together with grassroots activists, ordinary citizens, legal and data-protection experts. It was very interesting

and moving experience to work along with an ad-hoc group of activists which had consolidated to struggle against the government's initiative. The campaign used a variety of methods in a number of arenas: in hearing of the Science Committee at the Knesset (Israeli Parliament), which prepared the bill for the last vote, recruitment of public figures and renowned scientists to voice their opposition to the bill, media coverage, raising awareness and online activism and finally demonstrations. These tactics were aimed at pressuring Members of Knesset to oppose the bill.

One of the central arenas of the campaign was the hearings at the Knesset, where it was our assessment that changes to the proposed bill could be accepted. The hearings were also an opportunity to highlight the problems and risks expected from the establishment of a biometric database.

The parliamentary discussion regarding the bill was in fact the first time administration people, and their IT experts had to share the public with the details of the scheme and the set of considerations it derived from.

One of the most important lessons I have learned during the campaign, a lesson which I think can answer Prof. Rosen's question on the factors that may limit the success of campaigns against privacy invasive technologies, is the following insight:

IT projects, control technologies and surveillance systems, with severe consequences on human rights and democracy, are promoted without transparency.

They are planned and shaped in the bureaucratic burrows away from the public eye. They emerge in the Knesset and the public sphere only after their conceptual framework and architecture have been laid down; and plenty of resources have been spent in their infrastructure, sometime even in "pilots".

This mechanism leaves very **little room for a real debate in the Knesset and the public**. The Constitutional and moral discussion in the democratic sphere is taking place in the shadow of almost "fait accompli".

It is true that in the public administration there are many different vectors and interests, some are opposite to others. For example, if we were to take the legal team working in the public administration, these lawyers have two roles: one is to protect

democratic and constitutional values, which they did before the biometric initiative was brought to the knowledge of the public. For a long time they led an internal struggle, and even succeeded add some improvements in the scheme. However, once the high ranking officials succeeded to harness the ministerial rank to the “biometric carriage”, the internal opposition to the establishment of the database was overweighed. From now on the same team of lawyers had to take on their second role – as advocates of the government (and to assist the execution of the plans) to defend and promote the scheme in the Knesset in the public.

The end results being that when the issue became a public and democratic debate, the only serious and professional opposition that could challenge them was of the NGO’s and volunteer independent specialists.

The first conclusion I can offer today, is that we must make an effort to expose technological initiatives, which may either challenge, put at risk privacy and other human rights, at an earlier stage as possible, which will enable us to work towards public participation in the planning process.

Going back to the hearing held at the Knesset - The hearing was held at the “home filed” of the government. This is usually the case in our parliament, which enables bureaucrats to seek the help of the majority made of the coalition. This reality was especially illustrated, since the Minister of Interior, who promoted the bill inside the government, became now the head of the parliamentary committee to discuss the bill. As such, it is not surprising that he had stated at the beginning of the discussions that he has no intention to discuss the establishment of the database, only the details.

And yet, in a democracy, there is still the need for the “show” of the democracy, this show allowed a very narrow, yet important, leeway for activity. As I have explained, one of the goals of the activities in the Knesset was to cross-examine the representatives of the public administration and expose the dangerous and disproportional nature of their plane.

For example: during the discussions Members of Knesset were surprised to discover that even the Ministry of Interior experts had determined that the desired goals of the

database could be achieved without a “biometric” image database and the increased harm to citizens that it entailed.

The debate at the Committee had also led to some improvements in the details of the legislative arrangement to reduce the damage that will be caused by the database.

Here are a few examples: we succeeded in changing the bill, adding elements of

"Privacy by Design": for the first time we have legislation which instructs not only the way one should use the technological system but also the way the system should be designed. The scope of the circumstances, in which data would be transferred from the biometric database to the police, was reduced.

We succeeded to convince the committee to add a penal sanction in cases of leakage or misuse of the database even as a result of negligence. This change caused a remarkable discontent for the bureaucrats who advocated for the biometric database. They had assured that there was no fear of misuse or leak, but once the new sanction appeared they suddenly became much less determined and opposed it aggressively. In other words, they wanted all the power and authority, yet were tempting to avoid the responsibilities that come with that.

As for the focal point of the campaign: The campaign aimed and tried to prevent the establishment of a biometric database. But we couldn't afford ourselves to abandon the effort to reduce the damage to privacy in a case we would fail. Furthermore, we "resisted the biometric technologies entirely", but we concentrated our efforts on the database. That was a real-politics compromise, a tactical decision, based on the assumption that it would not be productive to lead an "all or nothing" campaign.

In the aftermath, I believe that we made the right decision, tactically, and that all in all the effort to improve protection of privacy did not compromise the effectiveness of the activity against the establishment of the database or the use of biometric technologies.

This is true, yet with some exceptions. We argued against the criminal sanction to anyone who refuses to provide a finger print, which was in the draft bill. Our case convinced decision-makers, and the sanction was dropped. It is possible that while

achieving this success we lost points in the awareness raising objectives of the campaign, because the sanction was only one manifestation, extreme and grotesque, to what would continue to exist regardless of the sanction: the actual biometric database – the taking of data from the human body is a violent invasion of the State to the privacy of the individual, which is made possible due to the power of coercion available to the authorities.

At this point I would like to relate to the public and media campaign. Probably, the most important lesson I have learned during the campaign is that we still have a long way a head if we wish to mobilize a mass movement against the "surveillance society". Explaining all the ramifications and risks that are part of careless use of IT is very complex. These messages are difficult to convey, especially in a "sound bite" interview in the media. When we began trying to explain this to the general public, we were surprised and frustrated to find out that the difficulties start from the basics – a lack of understanding of the internal and pragmatic value of privacy.

I am sure that all the participants of this conference today have vast knowledge on these issues. We, as members of the "privacy community" have access to many resources that allow us to know and understand. But we must find ways to pass on this knowledge and our insights to the public. I feel this is an important mission, perhaps even critical, to our goal to live as free citizens in a democratic society.

Thank you.

For further reading:

Nitzan Lebovic & Avner Pinchuk "The State of Israel and the Biometric Database Law: Political Centrism and the Post-Democratic State" [The Israel Democracy Institute](#).

Jonathan Klinger "We lost the skyline" [2jk.org](#) Dec 8, 2009

Jonathan Lis " MKs pass controversial bill to set up biometric database" [haaretz.com](#) Dec 8, 2009

David Shamah "The Biometric Law could make Israel a far less free society." [jpost.com](#) Dec 7, 2009

Ynet reporters "Knesset passes biometric database bill" [ynetnews.com](#) Dec 7, 2009

Amira Hass "Institutionalized voyeurism" [haaretz.com](#) Nov 24, 2009

Attila Somfalvi "Biometric database delayed by 2 years" [ynetnews.com](#) 17.11.09

Editorial "A hasty and destructive law" [haaretz.com](#) Nov. 16, 2009

Jonathan Klinger The Law Must Go On: Meir Sheerit's eagerness for the Biometric bill may be tainted [2jk.org](#) July 24, 2009

Campaign website - NO2BIO