



August 7, 2009

**DELIVERY BY COURIER**

Dr. Omer Tene  
P.O. Box 3112  
Karmey Yossef 99797  
Israel

Dear Omer:

It is timely that I write to you as the debate in Israel intensifies surrounding the proposed Biometric Documents Identification Law (Biometrics Law). Thanks to recent valuable consultation with you, my office now has greater insight as to the scope of the proposed Israeli legislation. I have also become increasingly involved in international biometric discussions. Specifically, I advanced the need for privacy to be paramount in the design of such systems.

Just yesterday I conducted an interview on biometrics with the leading global technology group, IEEE. My central message was this: As the use of biometrics becomes more widespread, so will the privacy and security risks associated with the growing collection, use, disclosure and retention of personal biometric data. These risks include: loss of individual control over one's personal information; unauthorized cross-matching, secondary uses (function creep), surveillance, profiling and discrimination based upon biometric data; and the loss, theft, misuse and abuse of this personal data, resulting in identity theft and other negative impacts on the individual.

As you know, large centralized databases of biometric personally identifiable information, linked to computerized networks, and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit. There are also significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.

The interview I mentioned above stemmed from a recent biometric discussion paper I produced with Max Snijder, my colleague on the European Biometrics Forum (see the paper enclosed with this letter). In a situation that echoes some of the privacy challenges facing Israel, Mr Snijder is currently actively opposing the acceptance of a new Netherlands law that allows biometric data captured on citizens' passports to be stored in a central national database. The database will be accessible by law enforcement to search the identity of persons suspected of committing serious crimes. The Dutch government is rightly facing heavy criticism for allowing personal

.../2



information to be used for a secondary purpose that goes well beyond the primary purpose of the collection; a back-door approach for gathering information if you will. I firmly believe that this represents a slippery slope towards evolving into a “police state” — it flies in the face of the fundamental understanding that privacy is an essential component of freedom and liberty.

I believe that the proposed Israel Biometrics Law would enable the government to create a database that would include biometric identification on every Israeli citizen. As is the case with the Dutch example, it is a regrettable reality that large centralized databases are also more prone to function creep and insider-abuse. I am heartened to learn that the government is now willing to “split” the database between two Ministries, but I would urge them to go even further.

When countries explore the use of biometric solutions for purposes of identity management and consider issuing electronic identity cards, privacy must be paramount in the design of such systems. My office always seeks to have privacy embedded into the design specifications of new technologies so that it is not viewed as a superfluous afterthought. I call this “Privacy by Design,” a term I developed in the ‘90s to capture the need for building privacy directly into the architecture of a given technology.

I genuinely understand the government’s need for setting up this program to protect public safety and national security, but within this scenario, the existing model of protecting privacy and safeguarding information invariably leads to a zero-sum game — where protecting privacy is believed to lead to less security. This need not be the case. This model must change from a “zero-sum” to a “positive-sum” paradigm where the need for privacy protection and the need for security may both be satisfied.

Enclosed is our Privacy by Design Principles, together with additional information on embedding biometric encryption capabilities to proposed biometric systems. These resources demonstrate the merits of Biometric Encryption (BE) to verify identity, to protect privacy, and to ensure security. The key message is that BE technology can help to overcome the prevailing zero-sum mentality involved with traditional biometrics, namely, that adding privacy to identification and information systems weakens security. By embedding BE technology into the system, you can have both privacy and security: you do not have to choose one over the other.

The promise of biometrics for secure digital authentication and ID management can only occur when the biometrics used are truly secure, and that is precisely what Biometric Encryption promises to deliver. Our office has long championed BE for the purpose of protecting privacy while achieving strong security. The real strength of BE lies in its application to 1:1 situations (where biometric information is compared against an individual identification item such as a passport). However, we believe that when combined with other, more conventional, biometric methodologies, BE can also play an important role in strengthening privacy controls within a 1:Many situation, such as a centralized database. We would be happy to explore the benefits of such an approach further with you.

The importance of BE was recognized recently by Professor Peter Swire who testified in Washington before the Senate Committee on Homeland Security and Governmental Affairs.

Their topic was "Protecting Personal Information: Is the [U.S.] Federal Government Doing Enough?" As part of his submission, Professor Swire recommended that the Committee ask for a report from key federal government offices, including the Department of Homeland Security and the Department of Justice, on the "biometric encryption" approach designed to use fingerprints and other biometrics with greater security and privacy. As Professor Swire noted, "The privacy and security advantages of this approach are large."

In support of this recommendation, Professor Swire referenced the BE work of our office at page 4 of his written testimony: "Fortunately, slightly more sophisticated biometric technology can greatly reduce these identity theft and other privacy risks. Dr. Ann Cavoukian, the Privacy Commissioner of Ontario, has been a global leader in promoting what is called Biometric Encryption. With biometrics expert Alex Stoianov, she has published: *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy.*" He also noted our work in his companion paper, *The ID Divide: Addressing the Challenges of Identification and Authentication.* Copies of these materials are enclosed for your information.

Adding the language of privacy into the deliverables of any biometric system is, in my view, essential, but rarely occurs. Therefore I would strongly encourage Israel to embed privacy into the design of any new system being contemplated, and Biometric Encryption to protect the databases. We would be happy to work with you or your government to expand upon these ideas.

I am also looking forward to "Privacy by Design: The Definitive Workshop" — the event that I am co-hosting with the Head of the Israeli Law, Information and Technology Authority, in Madrid on November 2, 2009. It will provide a wonderful opportunity to showcase the benefits of embedding privacy into the design of all technology to an international audience — I'm confident that Israel will be recognized for its leadership on this front.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Ann Cavoukian". The signature is fluid and cursive, with a long horizontal stroke at the end.

Ann Cavoukian, Ph.D.  
Commissioner

Enc.