

26th March 2007

Dear <Blank>,

Thank you for your letter explaining the situation regarding the library for KS1 and the system you intend to employ in tracking the children's borrowing.

However, I have serious concerns with regards to the method you are implementing and I feel I need to challenge this decision. Most parents would merely go along with this system out of apathy. I am not, however, one of them!

I am a software developer and work closely with colleagues around the world who deal with personal identity amongst other things. Ironically, its technologists such as myself (who stand to gain the most out of implementing these systems) that are the ones who come out most strongly against it!

I understand that you are complying with all the legal requirements in terms of its use. However, I am uncomfortable with my child's fingerprints being taken in **any** form, especially as it is being introduced without seeking consent from the parents. Compliance isn't the issue here though - it's moral. You are effectively storing the child's biometric readings which I find intrusive and, on the whole, unnecessary. Such a process has the effect of softening children up for such initiatives as ID cards and DNA testing in the future.

You have tried to re-assure the parents that it's not the actual fingerprint that is stored, but a '*number*'. Here are a few facts that you are not probably aware of:

- The short answer is that ***fingerprint templates*** are what are stored on these systems. These are the equivalent of fingerprints - rather like the difference between a drawing and a photo - otherwise the systems simply wouldn't work.
- Police, the security services, and governments use *fingerprint templates* to identify criminals.
- There are international standards to ensure that *biometric templates* from different manufacturers are compatible - so what's stored on one system can be read by any other, including government systems.
- Where *fingerprint templates* are stored in an encrypted form, it is impossible for anyone to guarantee that this won't be broken during a person's entire lifetime. A PIN number can easily be changed. A fingerprint, and the template derived from it, *cannot ever be changed*.
- In the future, *fingerprint templates* will be used to authenticate passports, bank accounts, etc. **Thus *biometric templates* are extremely valuable and need to be kept in a highly secure environment.**
- The US government's official National Science & Technology Council says you **CAN** reconstruct a fingerprint image from a *fingerprint template*.

So, technology such as this may appear benign, but your actions have long term ramifications that you cannot control or reliably predict. Once we start to accept this as the norm, we pave the way in future for further intrusions of privacy. This all may seem paranoid, but we are already 'sleep-walking' into a surveillance society and by accepting initiatives like this, we are taking another step towards that.

I also find it quite irresponsible that such actions have been taken without extraordinary consultation with all concerned. Any mechanised systems of identity demands governance and strict oversight by those being identified - that might mean parents demanding the fingerprints, social security numbers and passports of teachers to prevent abuse!

I would like to direct you to a couple of articles on the internet on the very system you intend to employ. They make interesting reading:

www.theregister.co.uk/2002/07/22/fingerprinting_of_uk_school_kids/
www.leavethemkidsalone.com

In fact, if you do a search on Google for 'School fingerprinting', you will find a plethora of articles on this very subject.

I would be grateful if you could tell me who in the school administration is **a recognised data integrity officer**? How do you intend to safeguard the data stored on this system from abuse? How secure is the environment where the data is stored? What steps will be taken to ensure other authorities cannot demand the data without warrant?

As a parent, I would need further clarification of the system being employed and would like you to demonstrate a need for such a system. If you can do without the technology, I urge you to take the lead and reconsider its use.

I'll leave you with a quote from Article 16 of the UN Convention on the Rights of the Child, which states "*no child shall be subjected to **arbitrary** or unlawful interference with his or her privacy...*"

Kind Regards,

Tarique Naseem