PET Quagmires

Gus Hosein

The way we argue...

Governments are too eager to implement technology that will never work.

TIME
IN PARTNERSHIP WITH CNN

Welcome to the Snooper Bowl

By LEV GROSSMAN

Happy, yelling faces. Red, drunken faces. Faces painted blue. Faces painted purple. Tens of thousands of faces--accompanied by plastic horns and giant foam hands--pouring into Raymond James Stadium in Tampa Bay last Sunday, ready to watch the biggest football game of the year. Meanwhile, someone--or rather, something--was watching them.

In a move that has been both hailed and decried, the Tampa Bay police department used the occasion of Super Bowl conduct a high-tech surveillance experiment unsuspecting guests. In total secrecy (but wit cooperation of the National Football League each of the games' 72,000 attendees were sc

RELATED ARTICLES

The Eyes (And Brain) Of The Beholder
Scientists used to believe that the human brain recognized faces as a whole. But a new study publish...

One More Cosmo - People
The ladies who introduced

c|net NEWS.com

Firm defends 'snooper bowl' technology

By Lisa M. Bowman
Staff Writer
Published: March 9, 2001, 12:40 PM PST

TalkBack | E-mail | Print | del.icio.us | Digg this

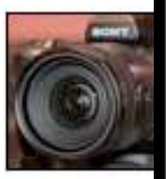
CAMBRIDGE, Mass.--To privacy experts, Super Bowl XXXV in Tampa, Fla., wasn't just a game--it was the "snooper bowl."

The event--where law enforcement captured the images of everyone entering gates of the Raymond James Stadium and compared them with a database of criminals' faces--ushered in the largest union of face recognition and video surveillance, according to civil liberties experts. They say that although the system was designed to ensnare terrorists and other criminals, it ended up nabbing only a handful of pickpockets and ticket scalpers.

"One has to question just how useful this was," said Barry Steinhardt, the associate director of the American Civil Liberties Union, speaking on a panel at the Computers Freedom and Privacy Conference 2001 here.

Privacy watchdogs are pointing to the game as the first massive example of biometrics abuse, warning that it could usher in an era where people's every move is tracked, from visits to the grocery store to auto travel.

But the chief executive of Viisage, the company behind the technology used at the Super Bowl, bravely faced the hostile crowd, defending his system as a protector of privacy instead of a violator.



Governments should design and implement technologies that promote the existing relationships in society, i.e. the status quo.

“Encryption, as a practical matter, diminishes the power of law enforcement to do its job, and we seek only the way to maintain the original status quo.”

- Janet Reno, Former Attorney General of the United States

Governments should design and implement technologies that promote data protection.

Information Commissioner

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 01625 545700
Fax: 01625 524510

e-mail: mail@dataprotection.gov.uk
Website: www.dataprotection.gov.uk

Mr John O'Brien
Micro Librarian Systems
1ST floor
Priory House
Ellesmere Avenue
Marple
Stockport
Sk6 7AN

Our ref : T0001

4th July 2001

Dear Mr O'Brien,

Thank you for taking the time to provide my colleague and I with a demonstration of **Identikit**, your biometric finger print recognition technology.

It is understandable that concerns will be raised over the use of such technology if it is believed that it involves the holding of a database of pupils' finger prints. However from what I understood of our discussions although theoretically possibly to use the information obtained from this system to match finger prints taken from a scene a crime, the resources this would require make this highly impractical. In light of this I do not believe that the use of the Identikit finger print technology to identify library members raises any data protection concerns.

Indeed since the system helps ensure the accuracy of the information held it aids compliance with the Data Protection Act 1998.

Yours sincerely,

Robert Mechan
Compliance Officer

Info Commissioner: Too late to stop school fingerprinting

Not that we really tried in the first place

By Mark Ballard → More by this author

Published Wednesday 17th January 2007 14:01 GMT

So many schools are taking the fingerprints of their pupils that it's too late to do anything about it, according to the Information Commissioner.

Yet the privacy guardian hasn't a clue just how many schools are taking children's fingerprints when they take registration, issue books from the library, or dish food out in the canteen (one supplier, at last count, had installed 3,500 systems). And the guidelines the Information Commissioner (ICO) promised nearly three months ago, which would reassure parents and instruct schools in the fine art of civil liberties, are still on the drawing board.

David Smith, deputy information commissioner, said: "For us to come out now and say fingerprinting isn't allowed would be very difficult because these systems have come in over the last four years. We were asked about them and we said it was okay." [Does that mean the government should un-ban handguns and hunting with dogs? *Ed*]

The ICO guidelines might now be written in collaboration with the Department for Education and Skills, he said, which is drawing up its own rulebook for school dabbers.

The preview the ICO gave *The Register* of its guidelines in September

Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Press Release

For immediate release

Date: 23 July 2007

Fingerprinting in schools

Schools that take pupils' fingerprints are being urged to properly consult parents and pupils and follow advice issued today by the Information Commissioner's Office (ICO).

Where fingerprints are taken, the data must be processed in line with the Principles of the Data Protection Act and the information can only be used for the specific purpose for which it was collected. Information should be processed on a suitably designed IT system, in which templates cannot readily be used by computers running other fingerprint recognition applications. High standards of security are required to safeguard the information and it should be destroyed when no longer needed.

Where a school intends to take fingerprints it should inform and consult pupils about the use of their personal information. A school should explain the reasons for introducing the system, how personal information is used and how it is kept safe. Some pupils – because of their age or maturity – may not understand the sensitivities involved in providing a fingerprint. Where a school cannot be certain that a child understands the implications of giving their fingerprint, the school must fully involve parents to ensure the information is obtained fairly. In circumstances where children are not in a position to understand, failure to inform parents and seek their approval is likely to breach the Data Protection Act.

The great danger is that key legal definitions like 'proportionality' and 'reasonable expectation of privacy' rely on the general mood of the public.

"In my view, whether privacy expectations are legitimate [within the meaning of Katz] depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."

- Justice Marshall dissenting in Smith v. Maryland

Assessing iTRACS

- Developing data mining systems
- Use in telecommunications, financial, and travel sectors
- Identity 'suspect' use and report to the authorities

Baseline

- Surveillance in homes?
- Intimate data?
- Interaction with protected communications?

DP Compliance

- Purpose specification?
- Require new legal basis?
- Less intrusive means available?
- Sensitive data?
- Linking, fusion or analysis?
- Anonymity removed?
- Regardless of being suspect of crime?
- Transparency regarding technology use?

Context sensitive trade-off?

- interfere with human dignity?
- interfere with physical integrity?
- aggravate judicial scrutiny?
- facilitate societal scrutiny?
- aim at crime prevention? prosecution?
- apply against terrorism? organised crime? random crime?
- increase security against state? in other spheres?

So, a useful exercise, but...

- How does this scale to outside the EU funding framework?
- Can we use this to assess government projects, and not those necessarily limited to security?

Concluding questions

Is it better to watch large systems be developed and fail, either in public opinion or technologically?

or,

Should we try to minimise the risk of failure by linking systems development to reality?

i.hosein@lse.ac.uk or gus@privacy.org

http://personal.lse.ac.uk/hosein

http://www.privacyinternational.org