Drawing a Blank:

The failure of facial recognition technology in Tampa, Florida

AN ACLU SPECIAL REPORT

By Jay Stanley and Barry Steinhardt

January 3, 2002

****

Introduction

Since September 11, facial recognition systems -- computer programs that analyze images of human faces gathered by video surveillance cameras -- are being increasingly discussed and occasionally deployed, largely as a means for combating terrorism. They are being set up in several airports around the United States, including Logan Airport in Boston, T.F. Green Airport in Providence, R.I., San Francisco International Airport, Fresno Airport in California and Palm Beach International Airport in Florida. The technology was also used at the 2001 Super Bowl, and plans are underway to use it at the NFL championship again in 2002.

The technology is not just being used in places where terrorists are likely to strike, however: in Tampa, Florida, it is also being aimed at citizens on public streets. Last summer, the Tampa Police Department installed several dozen cameras, assigned staff to monitor them, and installed a face recognition application called Face-IT® manufactured by the Visionics Corporation of New Jersey. On June 29, 2001, the department began scanning the faces of citizens as they walked down Seventh Avenue in the Ybor City neighborhood.

Acting under a Florida open-records law, the ACLU was able to obtain all existing police logs filled out by the operators of the city's face recognition system in July and August, 2001. Those documents and logs reveal several important things about the technology in one of its first real-world trials:

- The system has never correctly identified a single face in its database of suspects, let alone resulted in any arrests.
- The system was suspended on August 11, 2001, and has not been in operation since.

- In the brief period before the department discontinued the keeping of a log, the system made many false positives, including such errors as confusing what were to a human easily identifiable male and female images.
- The photographic database contains a broader selection of the population than just

things are really funny, like the way people dance when they think no one's looking. Others, you wouldn't want to watch."[3]

This technology has the potential to become an extremely intrusive, privacy-invasive part of American life. History shows that once installed, this kind of a surveillance system rarely remains confined to its original purpose. Already, in the case of face recognition, it has spread from purportedly looking for terrorists at the high- Åtchnri TD k

- camera locations
- the technical capabilities of the system being used
- the procedures, instructions and training provided to system operators

have also further reduced the chances that anyone in the database who wandered in front of the department's cameras would actually be identified by the software).

- Acting either on their own or at the direction of an internal policy decision, the officers operating the system decided to record only genuine matches, and not false positives. The log sheets are blank because there were no genuine matches.

Because the system does not automatically scan the faces of people on the sidewalks –

criminals, but anyone who might have "valuable intelligence" for the cop on the beat, according to these guidelines, will have his or her photograph entered into a police database so that they may set off an alarm whenever they visit a public place that is within the lens of a department camera.

The move to permanently brand some people as "under suspicion" and monitor them as they move about in public places has deep and significant social ramifications. If we are to take that path -- a step that the ACLU opposes -- we should do so as a nation, consciously, after full debate and discussion, and not simply slide down that road through the incremental actions of local police departments.

Conclusion

The documentary record obtained by the ACLU of the Tampa Police Department's experience with facial recognition technology adds an important new piece of evidence that the technology does not deliver security benefits sufficient to justify the Orwellian dangers that they present. What the logs show -- and fail to show -- tells us that face recognition software performs at least as badly in real-world conditions as it has in the more controlled experiments that have been carried out.

The only possible justification for deploying such an ineffective technology would be that it somehow deters crime because citizens believe that it works. There are several problems with that argument. First, it is premised on a Wizard of Oz-style strategy of hiding the truth about facial recognition technology from the public – a stance that is not compatible with the vital importance of public scrutiny of the tools, technologies and techniques that police departments deploy.

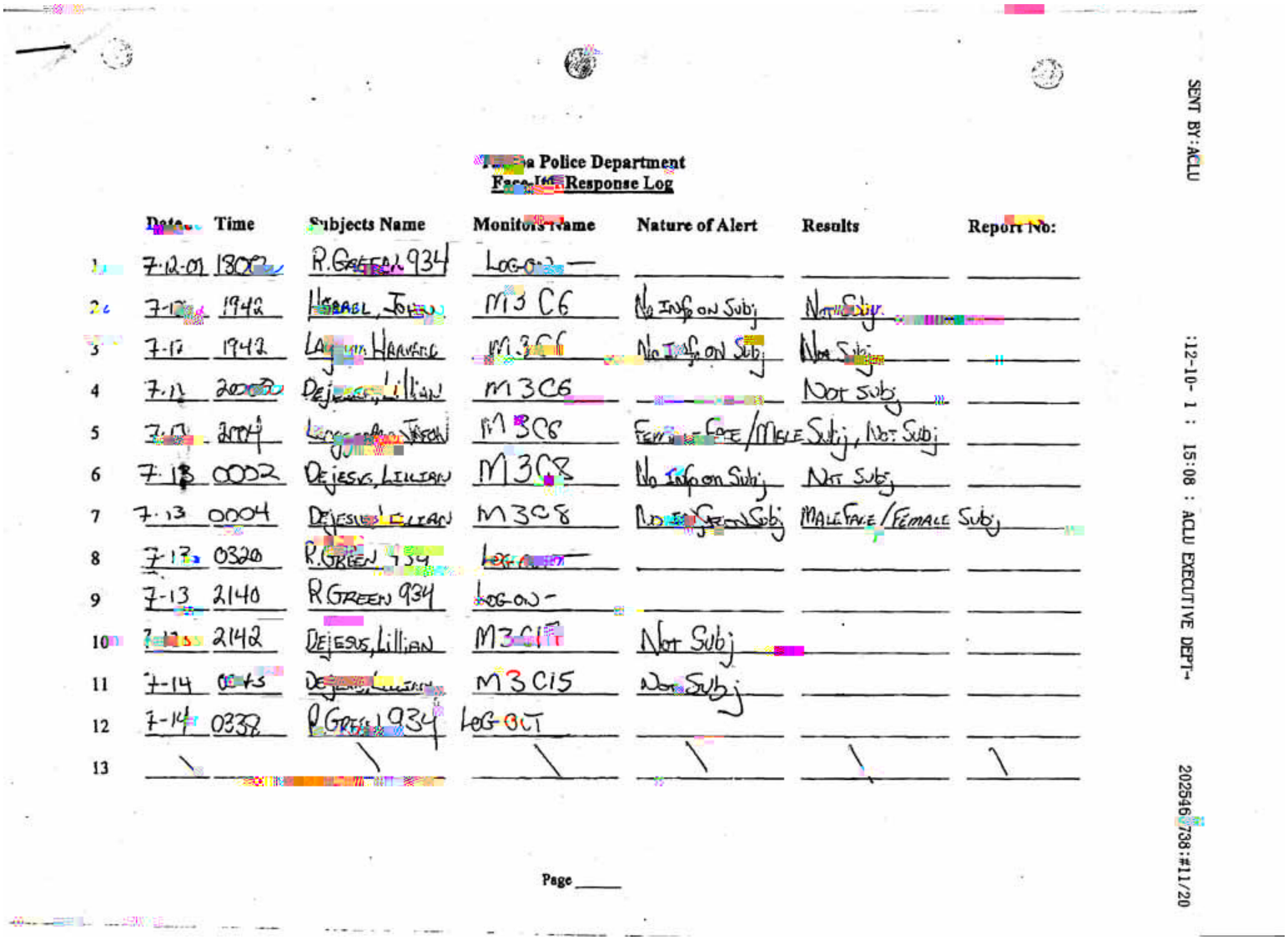
Second, even if face recognition cameras did deter wanted criminals from frequenting the areas under surveillance, all that would happen is that the criminals would move to other locations. Indeed, sociological studies of closed circuit television monitoring of public places in Britain – where residents are widely aware of the cameras – have shown that it has not succeeded in reducing crime.[10]

Given the system's poor performance in Tampa – which the police department there has implicitly recognized in their decision to stop actively using it – the ACLU hopes that police departments around the nation will step back, objectively examine the costs and benefits of the system, and reject them as ineffective. Other cities have voted to deploy these systems, including Virginia Beach, Palm Springs and Boulder City, Nevada. We ask those cities to consider the documentary evidence from Tampa and not waste precious resources on this illusory path toward public safety.

The worst-case scenario would be if police continue to utilize facial recognition systems despite their ineffectiveness because they become invested in them, attached to government or industry grants that support them, or begin to discover additional, even

[10] See http://www.scotcrim.u-net.com/researchc2.htm for the full text of the research findings of the Scottish Office Central Research Unit.

1-1 One of the Tampa Police Department log sheets showing false positives generated by face-recognition system.

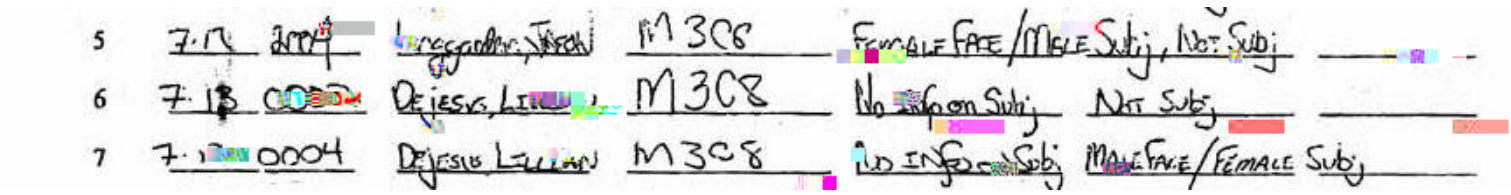


Police Department
Face Response Log

	Date	Time	Subjects Name	Monitors Name	Nature of Alert	Results	Report No:
1	7-12-01	1802	R. GREEN 934	LOG-ON			
2	7-12	1942	HARRIS, JOHN	M3 C6	No Info on Subj	Not Subj	
3	7-12	1942	LAST NAME HARRIS	M3 C6	No Info on Subj	Not Subj	
4	7-12	2000	DEJESUS, LILIAN	M3 C6		Not Subj	
5	7-13	2004	LAST NAME JOHN	M3 C8	FEMALE FACE / MALE	Subj, Not Subj	
6	7-13	0002	DEJESUS, LILIAN	M3 C8	No Info on Subj	Not Subj	
7	7-13	0004	DEJESUS, LILIAN	M3 C8	No Info on Subj	MALE FACE / FEMALE	Subj
8	7-13	0320	R. GREEN 934	LOG-ON			
9	7-13	2140	R GREEN 934	LOG-ON			
10	7-13	2142	DEJESUS, LILIAN	M3 C15	Not Subj		
11	7-14	0043	DEJESUS, LILIAN	M3 C15	Not Subj		
12	7-14	0332	R GREEN 934	LOG-OUT			
13							

Page ____

1-2 Many of the false positives made by the system were to a human observer obvious mismatches. Here we see logs indicating that the suspect was of the opposite sex from the person in the database.



1-3 Although several log sheets listed false positives, most of the sheets were blank. And this one, from August 11, is the last log showing that the system

Tampa Police Department

FACE-IT SYSTEM LOG

Operator D.H. Walker P/R # 43051 Date/Time In 8-11-01 /2200 Date/Time Out 8-12-01 /0600

Date/Time	Location of Activity/Stop	Camera #	Contact's Name	Nature of Contact	Report #	Comments (Valid or Invalid Alert)
N/A						

SENT BY:ACLU ;12-10- 1 ; 15:12 ; ACLU EXECUTIVE DEPT→ 2025460738;#2