Being Audience Rating – Data Protection

Summary of Relevant Data Protection Considerations

Being Audience Rating (BAR) solution uses images from Behavior Tracking Sensor and a suite of proprietary real-time image processing algorithms to:

- detect the presence of human faces in the digital images provided by the sensor;
- perform a tracking of each detected person while they remain within the sensor's field of vision;
- optionally assign a set of anonymous qualifying tags to each tracked person, such as gender or age information.

BAR converts video images into a set of abstract numeric descriptors such as the current number of viewers and their dwell time. User privacy is fully respected since:

- the abstract numeric descriptors constitute aggregate anonymous data;
- image processing takes place in real time and at no point in the processing chain is the visual information stored on non-volatile memory or relayed elsewhere.

BAR solution is used in public places for audience measurement, content adaptation and interactivity purposes; venues include commercial centers, shops, agencies, services, and transportation networks. The purpose of this document is to demonstrate that BAR solution complies in full with current legislation concerning the protection of personal data.

Acer Being Signage
Being Audience Rating

Using Behavior Tracking Sensor to analyze customer behavior

1 Non-Persistency of Video Images

A digital video frame, as captured by a sensor, is relayed to the processing unit running BAR as a stream of binary digits. The physical layer is usually a USB connection. The video image is stored in RAM (volatile memory) for the time necessary for analysis and processing; this time is dependent on the computing platform but is comprised between 66 and 200 milliseconds. The volatile storage area in which incoming digital images are stored is overwritten each time a new image is delivered thereby erasing all trace of previous visual information. As a consequence, no visual snapshot as is remains in the system for more than a few hundred milliseconds.

BAR, as most image processing systems, employs longer-term processing for computer vision tasks such as background extraction and motion estimation. These algorithms rely on long-term averages of video information which, by definition, are fully static and do not contain any information which could be used to visually identify people or activities.

BAR solution is not a video surveillance system: it does not record any video files and no video feedback is provided to an external operator during use.

The key point is that the information generated by BAR solution cannot be considered “personal data”. The definition of “personal data” can be found in various pieces of legislation; for instance, it is defined by the European Directive 95/46/EC as "information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;".

2 Anonymity of BAR Data

BAR solution produces the following set of completely anonymous data for each detected person:

counter	is a sequential number for the data record
machine_ ID	is the identification number for the machine processing the data
start_time	is the date and time of the initial detection
presence	is the amount of time the person remains within the senson‘s field of vision
attention	is the amount of time the person has been looking at the object of interest
gender	[optional] is the person’s gender
age	[optional] is the person’s age bracket
distance	is the person’s latest distance from the object of interest
num_glances	is the number of glances during the viewing session

No face database based on visual characteristics is created during use either so that the system does not recognize recurring appearances of the same person. In other words, the system permanently “forgets” detected people as soon as they leave the sensor’s field of view.

In conclusion, BAR solution uses advanced image processing techniques to provide non-identifiable and non-visual information to databases and devices, for marketing purposes.

ISO 27001 Certificate

bsi.

By Royal Charter

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: Acer Cloud Technology (Taiwan) Inc.
8F.
No. 88. Sec. 1, Xintai 5th Rd.
Xizhi Dist.
New Taipei City
22181
Taiwan

Holds Certificate No: **IS 641261**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The provision of Acer Build Your Own Cloud (BYOC) operation including system management, network management, supplier management, incident management, change management, customer service level management, and related security processing activities by Platform Operation & Management Division.
This is in accordance with the Statement of Applicability, ISMS-201-04, Ver. 1.3, dated 20 Dec. 2016.

For and on behalf of BSI:

Chris Cheung, Head of Compliance & Risk - Asia Pacific

Original Registration Date: 03/02/2016
Latest Revision Date: 26/12/2016

Effective Date: 03/02/2016
Expiry Date: 02/02/2019

...making excellence a habit.™

HIPAA Compliance Report

1 Assessment Purpose

The purpose of this assessment was to assess the security controls against HIPAA security rules, in place with respect to the provision of Acer Build Your Own Cloud (BYOC) operation including system management, network management, supplier management, incident management, change management, customer service level management, and related security processing activities by AOP Platform Solution & Operation Div. The findings identified are based on the HIPAA Security audit procedures addressed by the U.S. Department of Health & Human Services (see "HIPAA Securirty Assessment Report"), information obtained from interview with Acer BYOC AOP supervisors and key personnel, observation of security controls, sampling of operation records, and review of the Information Security Management System SOPs.

2 Impact Indicators

Findings and recommendations are provided in the "HIPAA Security Assessment Report". Each finding is marked as Major, Minor, or OFI (Opportunities For Improvement) within its Impact section, indicating the degree of how this finding may impact the security management of electronic Protected Health Information (ePHI). The degrees of the different impact indicator are as described below:

Major – The finding may cause most of the security management of the ePHI ineffective, which may result to severely compromise the security of the ePHI.

Minor – The finding may cause some of the security management of ePHI less efficient. If many minor findings are not treated appropriately within the organization, it may compromise the security of the ePHI.

OFI – The finding may not cause any specific security management domains of the ePHI to be inefficient. However, this is not regarded as a good practice in the industry.

The security rules assessed during the course of the visit were found to be effective. There were no major findings in this assessment.

KPMG
cutting through complexity