Facebook Custom Audiences Product

Report on Management's Assertion over Custom Audiences security controls as of August 21, 2013

Facebook, Inc

This report is intended solely for the information and use of Facebook and users of Facebook's Custom Audiences product, defined as Advertisers who have read the Custom Audiences Terms. The report is not intended to be and should not be used by anyone other than these specified parties.

Table of Contents

1 Report of Independent Accountants

Report of Independent Accountants

[Scope]
We have examined management's assertion: that as of August 21, 2013, Facebook Inc. ("Facebook") have established specified control objectives ("criteria") and related controls to achieve the following assertions:

- A: The information provided to Facebook by advertisers for the matching process in the Custom Audiences product is not shared with other advertisers or third-parties;
- B: Facebook has implemented safeguards that are designed to (a) protect the security and integrity of data while it is within Facebook's systems and (b) guard against the accidental or unauthorized access, use, alteration or disclosure of data within Facebook's systems; and
- C: The information provided to Facebook by advertisers to facilitate the creation of Custom Audiences is retained for only as long as needed for the matching process to complete. Facebook appropriately disposes of such information once it is no longer required for the matching process.

Facebook's management is responsible for the assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

[*Inherent limitations]*
Our examination was limited to examining the specified control objectives and related controls and did not consider any other control objectives or controls that may be relevant to management or the users of the Custom Audiences product. The effectiveness of controls to achieve the specified control objectives is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection to the future of any evaluations of effectiveness or any conclusions about the suitability of the design of controls to achieve the related control objectives is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations.

[*Other information provided by Company]*
The information included in Section 4, "Other Information Provided by Facebook (unaudited)", is presented by management of the Facebook to provide additional information and is not a part of management's assertion. Information about the Facebook's description of the custom audiences product has not been subjected to the procedures applied in the examination of management's assertion and of the suitability of the design of controls to achieve the specified control objectives stated in management's assertion and accordingly, we express no opinion on it.

PricewaterhouseCoopers LLP, 488 Almaden Boulevard, Suite 1800, San Jose, CA 95110
Telephone (408) 817 3700, Fax (408) 817 5050, www.pwc.com

[*Opinion]*
In our opinion, management's assertion referred to above is fairly stated, in all material respects, based on the control objectives established by management set forth in Section 3 Description of Custom Audiences Control Objectives and Controls .

[*Restricted use]*
This report is intended solely for the information and use of Facebook and users of the Custom Audiences product and is not intended to be and should not be used by anyone other than these specified parties.

Pricewaterhouse Coopers LLP
San Jose, CA
September 16, 2013

PricewaterhouseCoopers LLP, 488 Almaden Boulevard, Suite 1800, San Jose, CA 95110
Telephone (408) 817 3700, Fax (408) 817 5050, www.pwc.com

2 Management Assertion over Facebook's Custom Audiences Product

facebook

Management's Assertion

Facebook provides the Custom Audiences product to allow advertisers to create specific targeted audiences from their data. As it relates to the information transmitted by advertisers to Facebook for use of the Custom Audiences matching process, we, as members of management, have established a Custom Audiences Terms of Service document ("Custom Audience Terms") that states, in part, the following are performed to protect the security of data transmitted to Facebook for use of the Custom Audiences process:

- A: The information provided to Facebook by advertisers for the matching process in the Custom Audiences product is not shared with other advertisers or third-parties;
- B: Facebook has implemented safeguards that are designed to (a) protect the security of data while it is within Facebook's systems and (b) guard against the accidental or unauthorized access, use, alteration or disclosure of data within Facebook's systems; and
- C: The information provided to Facebook by advertisers to facilitate the creation of Custom Audiences is retained for only as long as needed for the matching process to complete. Facebook appropriately disposes of such information once it is no longer required for the matching process.

For each of the assertions, management has established specified control objectives ("criteria") and related controls. These criteria and related controls are the responsibility of Facebook and are presented in *Exhibit A – Description of Custom Audiences Control Objectives and Related Controls.*

We have evaluated whether Facebook's controls were suitably designed to achieve the specified control objectives as of August 21, 2013. The controls were evaluated against the criteria included in *Exhibit A – Description of Custom Audiences Control Objectives and Related Controls*. Based on our evaluation, management asserts that:

- The controls for the Custom Audiences Terms as stated above, that are presented in *Exhibit A – Description of Custom Audiences Control Objectives and Related Controls* were suitably designed as of August 21, 2013 to provide reasonable assurance that the specified control objectives were achieved.

By: _____

Joe Sullivan

Chief Security Officer

1601 S. California Avenue, Palo Alto, CA 94304
650.543.4800 - tel 650.543.4801 - fax

Exhibit A - Description of Custom Audiences Control Objectives and Controls

Control objective 1: Hashing of personally identifiable data elements

Controls provide reasonable assurance that personally identifiable data elements[1] (email addresses and phone numbers) sent to Facebook are protected through the use of the SHA 256 cryptographic hashing function.

Control #	Control activity
1.1	Custom Audience personally identifiable data elements (email addresses, phone numbers) submitted through Power Editor are automatically hashed in the browser as part of the Power Editor upload process.
1.2	Custom Audience data (email addresses, phone numbers, Facebook user IDs) submitted through the API or Power Editor undergoes the following validation checks to ensure plaintext data is not processed and stored: ▪ Data submitted that contains the "@" symbol will be rejected and will not processed or stored. ▪ Data submitted that contains a "(" or "-" symbol will be rejected and will not be processed or stored. ▪ Data submitted that is not within an expected range of Facebook user ID numbers will be rejected and will not be processed or stored.

Control objective 2: Protection of data in transit over the internet

Controls are in place to provide reasonable assurance that Transport Layer Security (TLS) is configured using leading industry practices to protect transmitted data, including the hashed data elements, when being sent to Facebook over the Internet.

Control #	Control activity
2.1	The Facebook API servers that receive and process Custom Audience data are configured by Facebook with TLS encryption.
2.2	The only channels that Custom Audience data (email addresses, phone numbers, Facebook user IDs) can be received by Facebook are the API or Power Editor.
2.3	Digital Certificates used to provide the TLS encrypted connection between Facebook and the user's browser are from a WebTrust Certified Certificate Authority, and are not expired.

[1] There are three types of data elements that can be submitted through the Custom Audiences product; email addresses, phone numbers and Facebook user IDs. Email addresses and phone numbers are defined as personally identifiable data elements, Facebook user IDs are not defined as personally identifiable data elements.

Control objective 3: Usage, storage and retention of Custom Audience data

Controls are in place to provide reasonable assurance that measures are taken by Facebook to a) limit the use of hashed data elements; and b) process and store the data for the minimum amount of time to ensure completion of the Custom Audience transaction and c) permanently deleted data after matching process completes.

Control #	Control activity
3.1	Submitted and hashed Custom Audience data is not stored outside of the specific data store that is necessary for the processing of the matching. Custom Audience data within this data store is not processed by any other system outside of the Custom Audiences matching process.
3.2	User data provided by advertisers that will be hashed (email addresses and phone numbers) does not exist in plain text format within the Custom Audience data store in the Facebook environment.
3.3	Custom Audience import activity, including access to data, is logged.
3.4	The Custom Audience data store is configured to automatically remove customer-provided hashed data after the period of time needed for the audience creation process to complete, which is defined as up to 2 days.

Control objective 4: Sharing of Custom Audiences

Controls are in place to provide reasonable assurance that customer generated Custom Audiences are associated with the Customer's Ad Account and are not visible to other advertisers unless explicitly shared.

Control #	Control activity
4.1	Custom Audiences are associated with only the Customer's Ad Account that created/owns the account unless explicitly shared by the custom audience owner.
4.2	The Custom Audience owner has access to modify, delete or share the Custom Audience and such access isn't available to any other advertisers.

Control objective 5: Security vulnerability assessment

Controls are in place to provide reasonable assurance that security vulnerabilities within the Custom Audiences system are identified and remediated.

Control #	Control activity
5.1	Power Editor and the Ads API are periodically penetration tested by a qualified 3rd party and any significant vulnerability identified during 3rd party reviews is remediated.

Control objective 6: Access to systems and data

Controls are in place to provide reasonable assurance that access to relevant components of the Custom Audiences system are restricted to only authorized personnel.

Control #	Control activity
6.1	Facebook has an Information Security Policy which is reviewed periodically and available to all employees.
6.2	New user access to privileged systems and groups is requested through a provisioning tool with an automated workflow. System owners authorize the nature and extent of user access privileges prior to granting access.
6.3	Role-based user access is controlled through the use of LDAP groups. If a user switches departments within Facebook, an alert is triggered and will be reviewed by Facebook Security to determine if the level of access (based on the groups the user is assigned to) is commensurate with their new job responsibilities.
6.4	Termination of employee access is an automated process performed through an Identity Management Termination Tool. Terminated users' access is automatically de-provisioned from any systems in which they had access upon the date of their termination, including: ▪ Internal Portal ▪ Active Directory ▪ Unix (if applicable)
6.5	Access to Custom Audiences' production environments is controlled using two factor authentication and a PKI system.

Control objective 7: Change management

Controls are in place to provide reasonable assurance that updates, changes, and configuration of Custom Audiences' systems are tested, reviewed and authorized prior to implementation.

Control #	Control activity
7.1	All changes to the Custom Audiences' infrastructure and back-end environment follow the Facebook coding and release process. All code changes are peer-reviewed and tested prior to releasing to production.
7.2	Access to release code into the production environment is restricted to authorized personnel only.

3 Other Information Provided by Facebook (unaudited)

Facebook's Description of the Custom Audiences Product

Facebook's Custom Audiences is an advertising tool that allows advertisers the ability to target specific user groups based off data the advertiser already has, such as email addresses, phone numbers, or Facebook user IDs. The tool allows these data sets to be uploaded to Facebook's servers, and matched with existing accounts to create targeted segments of specific Facebook users.

The mechanism for creating audiences is through an internally developed web interface called Power Editor. Audiences are also able to be created through the Ads Manager API. Facebook has implemented certain controls and security mechanisms to protect and secure uploaded advertiser data including specific controls within the matching process and restrictions on data retention and usage

The process has been designed to cryptographically hash customer data that advertisers have independent of Facebook (such as telephone numbers and email addresses) prior to any information being received by Facebook. JavaScript code within the browser hashes the information, and it is passed to Facebook through the Ads API. The hashed data is then matched against hashed Facebook user data to determine if the corresponding accounts exist. The resulting output of matching accounts is called a "Custom Audience." The Custom Audience does not list any specific user data, nor does it identify for advertisers specifically which users successfully matched. Rather, user information for advertisers is organized into aggregate demographics, describing the audience as a whole. For example, the Custom Audience attributes list an approximate number of matches, rather than the specific individuals included in the Custom Audience. Furthermore, access to the Custom Audience by an advertiser does not include access to Facebook unique identifiers, such as user ID, nor do the data sets contain other information about users in the Custom Audiences. The data set is linked to a consumer using only the Audience ID – a number assigned to each new Custom Audience, used by Facebook as a dataset identifier. Facebook does not keep data (matched or unmatched) provided by the advertiser, except for the time necessary to properly perform the match. After that, Facebook destroys the advertiser provided data.

Facebook's Description of the Custom Audiences Processing and Related Controls

Getting Started and Accessing Custom Audiences

1. ***Accessing the Power Editor for Custom Audiences***
   The first way that customers can submit data for the creation of a Custom Audience is using Power Editor. This can be accessed via the customers Ad Manager page. Customers download all their current Ads Account data into Power Editor in order to manage the account and its associated Pages.

2. ***Gaining access to the Ads API***
   The second way to create and manage Custom Audiences is through the Ads API. In order to have access to make the Ads API calls, advertisers may partner with "Preferred Marketing Developers" ("PMDs") – they have elevated access given to specific strategic ad partners to enable this functionality. PMDs have API keys used for authentication, before the API will respond to requests.

Creating Custom Audiences

1. ***Uploading and submitting data through Power Editor and the API***
   Power Editor is a web application that sends data to Facebook via the Ads API. Regardless if the advertiser's PMD is directly calling the API, or using the GUI (Power Editor) themselves, the commands to the API are the same; and funnel through the same entry point. Customers can submit data in either .txt or .csv formats. The application will match on emails, UIDs, or phone numbers.

2. ***Hashing client-side customer provided data***
   Email addresses and phone numbers are hashed *prior* to being sent to Facebook. The hashing always takes place on the client side. When uploading data using Power Editor, JavaScript within the browser is used to execute the hashing. Advertisers that use PMDs are also able to send information directly to the Ads API, bypassing the Power Editor user interface. However, because sending API commands do not include the inherent hashing functionality used by Power Editor when advertisers' PMDs submit data to the API directly, they are responsible for inputting the hashing syntax in the API command.

3. ***Data validation***
   Facebook limits the data that can be processed to create Custom Audiences, by including data validations within Custom Audiences' web server. Facebook stores only the data that passes the validations. Checks for inappropriately formatted data are performed prior to processing. Facebook performs the following data validations for Custom Audiences' customer input files:
   - Data submitted as Facebook userIDs are validated to ensure that they are numbers only, and no additional characters (such as: "@", ",", or "-") are included in the string.
   - Data submitted as email addresses will not accept values that do not have the "@" symbol.
   - Data submitted as phone numbers will not accept values that have the "(" or "-" symbols.

Matching Audience Data against Facebook Users.

1. ***Facebook hashing and matching capabilities***
   Facebook hashes user account data in the same way advertisers hash their data. This allows Facebook to perform a matching process against the advertiser provided data, and determine which users in the advertiser provided data have Facebook accounts. Facebook uses a proprietary multivariate matching process that allows them to match data based off multiple criteria. Custom Audiences can utilize multivariate matching in the event that the customer provides multiple variables for each user in their dataset. This can also be done by specifying the parameters of the campaign and audience the advertiser wants to target within their Ad Manager.

2. ***Matching advertiser provided data with Facebook users***
   The hashed advertiser provided data is sent through the Ads API to Facebook for further validation. These validations check to make sure the data is formatted properly and that plaintext data is rejected with an error message.

   The validated data is then compared to Facebook user data, and matches are identified to create the Custom Audience for the Advertiser.

   It is important to note that this process is asynchronous and as a result, the Custom Audience can take up to two days to generate (depending on the size of the audience) and be sent back to the customer.

Data Protection and Deletion

1. ***Retention of data by Facebook***
   All hashed advertiser provided data is removed once the asynchronous matching process is complete. The retention period can last up to 48 hours. This duration is considered by Facebook Engineering to be the maximum amount of time required to successfully process any Custom Audience. After that time, the hashed advertiser provided data is removed permanently. Additionally, any attempt to query or access the Advertisers' hashed data is logged.

   Only privileged users have access to the environment where Custom Audience data is stored. Once the data is matched and the audience is created, the hashed data is not used for any other purpose, destroyed and not accessible from Facebook systems.

Sharing of Custom Audiences

1. ***Sharing between ad accounts***
   Custom Audiences, by default, are only visible by the Facebook user account that created them. The Custom Audience owner can share their audiences by using Power Editor or by making an HTTP POST request within the API. The Custom Audience owner specifies the Ad Account ID of the user(s) to whom want to share the Custom Audience. Custom Audience owners are able to share their audiences with as many other ad account users as they wish. Additionally, at any time, the sharing privileges may be revoked by the Custom Audience owner.

2. ***Shared account access privileges***
   After Custom Audiences are shared between users, the user with whom the Custom Audiences has been shared does not have the ability to modify, delete, or further share the audience; nor could the information about the Facebook users within the Custom Audience be viewed. Only the user that created the Custom Audience may edit or share it.

Managing Access to Related Systems

1. ***Access management for privileged and non-privileged systems***
   Access to production systems housing the customer provided hashed data is restricted to Facebook authorized personnel that need it. Additionally, access to the development environment requires 2-factor authentication.

2. ***Facebook accounts***
   Authentication to internal web-based tools is restricted to the employee's individual Facebook account. When an employee performs certain actions, whether it is developing code, responding to incident requests, or logging on to a specific system, the action is attributed to an easily traceable account.

3. ***Changes and termination of access***
   In the event an employee transfers roles within the organization, an automated alert is sent to the employee and the information security team for review. The Security Engineer reviews the change and communicates with the transferred user to make a determination as to whether any subsequent system access changes need to be made.

   Facebook utilizes an Identity Management tool to automatically de-provision user access to all systems in the event of their termination. This tool interfaces with the HR system of record, which indicates a change in the user's employment status. As a result, the automated tool removes the user's access from all systems, including physical building access.

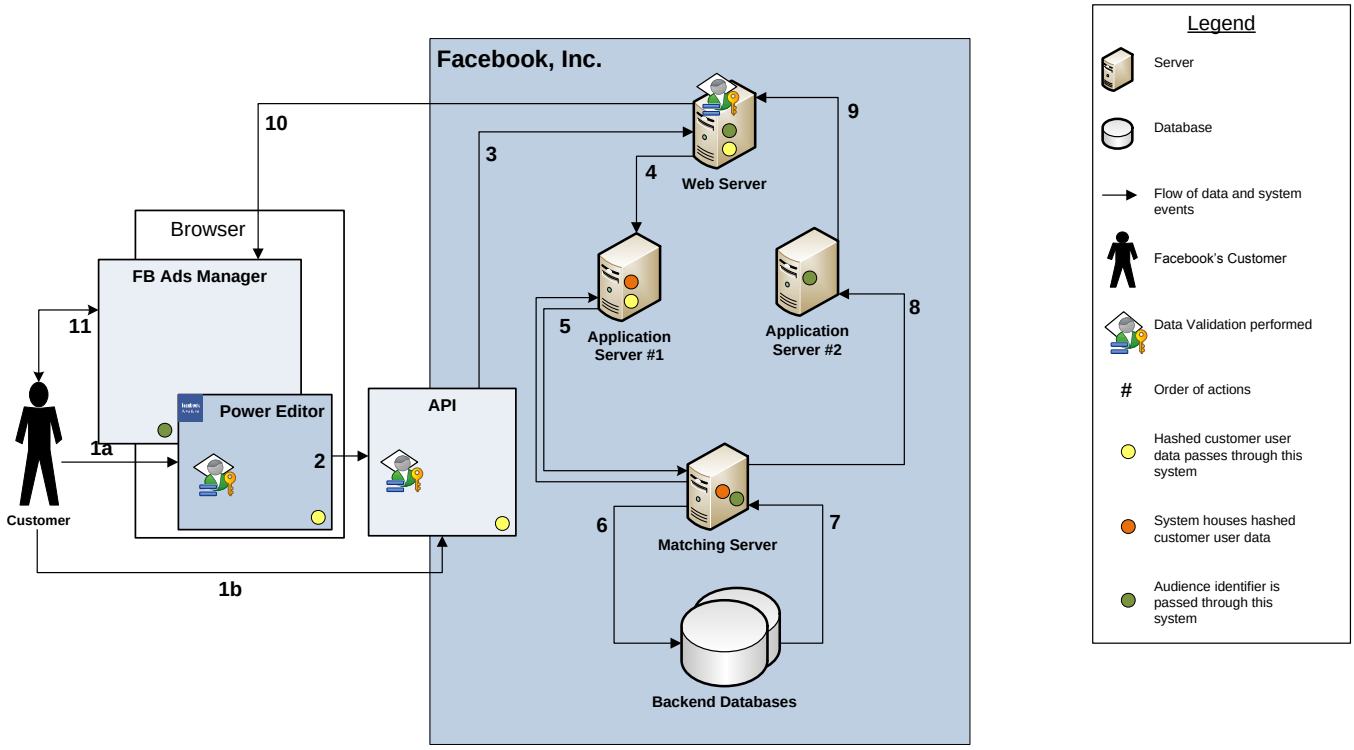
Managing Changes to Related Systems

1. ***Change and configuration management***
   Changes to the Custom Audiences' infrastructure and back-end environment, including operating systems, databases, servers, and interfaces, follow the Facebook coding and release process. This process includes documentation, enterprise-wide consistent secure coding practices, peer level code reviews and testing, segregated environment access restrictions, and a formalized code release process.

2. ***Change documentation and review***
   Changes submitted and released to production are automatically captured within the source-code repository and Facebook release libraries. The process is designed to require multiple users to review and authorize the change before it can be released into production. All committed code changes are reviewed by an individual that is different than the developer, and are tested prior to commit to production. A history of every change made to a specific system or code base is captured and available for review.

3. ***Releasing changes to production***
   Facebook has a defined code release process. Access to release code to the production environment is restricted to only the engineers with responsibility and authority to release changes. The release team will not release code to production unless adequate testing has been performed and all changes have been approved for release into production.

Custom Audiences Environment Overview



Process Descriptions

1a. The advertiser uploads their user data to Power Editor.
1b. The advertiser sends their user data to the API. The customer is responsible for hashing the data, using their API command.
2. Power Editor hashes the user data input, and sends it to the API.
3. API sends the hashed data to a Facebook Web Server to redirect the data internally.
4. The hashed data is written to an internal Facebook server [Application Server #1].
5. Matching Server asks Application Server #1 if it has any new data – if so, it will grab the new hashes.
6. Matching Server then performs a match of the customer data and sends the matched hashes to Backend Databases.
7. Backend Databases send back the corresponding Facebook user data to the Matching Server.
8. Matching Server creates an identifier for the new audience, then sends the ID to Application Server #2.
9. Application Server #2 sends the audience identifier back to the Web Server.
10. The Web Server sends the audience identifier (which links to the audience's metadata) back to the Facebook Ads Managers page.
11. The customer is then able to view and interact with the audience they have created.