Mobile App Advertising Guidelines
A Framework for Encouraging Innovation While Protecting User Privacy
June 2012
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highlights</td>
<td>3</td>
</tr>
<tr>
<td>Introduction: Why Mobile App Advertising Guidelines</td>
<td>3</td>
</tr>
<tr>
<td>Guidelines Definitions</td>
<td>4</td>
</tr>
<tr>
<td>Guidelines at a Glance</td>
<td>4</td>
</tr>
<tr>
<td>Transparency and Clarity</td>
<td>7</td>
</tr>
<tr>
<td>Enable Individual Control</td>
<td>10</td>
</tr>
<tr>
<td>Ad Delivery Behavior</td>
<td>11</td>
</tr>
<tr>
<td>Focused Data Collection</td>
<td>14</td>
</tr>
<tr>
<td>Transport Security</td>
<td>18</td>
</tr>
<tr>
<td>Conclusions &amp; Next Steps</td>
<td>19</td>
</tr>
</tbody>
</table>
HIGHLIGHTS

- The mobile ecosystem is innovating at a rapid pace, as it continues to evolve it’s important that standards are developed to ensure that the mobile ecosystem can continue to thrive while private user data is accessed and managed appropriately.

- The Mobile Ad Guidelines hope to establish a set of mutually agreed upon standards and guidelines to help those building and integrating in-app mobile ad technology.

- At-a-glance, the guidelines cover requirements and suggested best practices around transparency and clarity of data collection, individual control over information collected, ad delivery and display behavior, collection and retention of personal or device-specific data, and secure transport of sensitive data.

- Implications of these guidelines would require the following of ad providers:
  - Provide comprehensive, readable privacy policies and related FAQs to their app publishing partners, making educated integration easier for app developers
  - Provide a conspicuous notice to users and gain explicitly informed consent from within the mobile app if the ad provider intends to access personal information like phone number, email and name.
  - Provide clear attribution to the host application for ads that appear out-of-app. Ad providers that modify browser settings or add an icon to the mobile desktop must provide conspicuous forms of notice to users and gain explicitly informed consent before such behavior is triggered.
  - Move away from using permanent, unchangeable device identifiers and move towards using independent and/or temporal device identifiers that provide the same level of functionality with respect to targeted advertising.
  - Do not collect device identifiers that are tied to mobile subscriber identities unless the collection of such identifiers enables a demonstrable feature or service for the user.
  - Securely transport personal information, including device identifier data and personal information.

INTRODUCTION: WHY MOBILE APP ADVERTISING GUIDELINES

Mobile devices - and the apps contained within them - are increasingly “always on,” collecting valuable information such as location, communications records, social circles, and browsing preferences. In many ways, this information is the lifeblood of the mobile ecosystem: not only can it be coalesced to deliver incredibly informative, relevant, and delightful experiences for mobile users, but it can provide value to mobile advertisers to help fuel the mobile economy.
The importance of ad revenue in technological innovation cannot be understated. It fuels search giant Google and makes thousands of free applications and services possible. While this concept is fairly well understood by users of larger, more popular products and services, it’s often less clear that these same relationships exist for large and small businesses alike: up-and-coming mobile App Publishers looking to monetize their apps are often reliant on the same business model that Facebook uses, only without the massive userbase. The result is even more pressure on mobile developers and publishers to make their ads as valuable as possible.

Consequently, some advertisers have begun to experiment with aggressive new techniques for delivering targeted mobile ads or gathering increasing amounts of user data from mobile devices. Given the pace at which the mobile ecosystem is moving, it’s important that standards are developed to ensure that private user data is accessed and managed appropriately, and that controversial behavior is properly highlighted.

The intent of this document is to establish a set of mutually agreed upon guidelines to help those building and integrating in-app mobile ad technology to understand what is acceptable, and what is not. Each of the participants in the mobile ecosystem - Ad Providers, App Publishers and end users - has a role to play in the establishment and enforcement of these guidelines. Our hope is that they will result in a mobile ecosystem that is self-regulatory in nature.

GUIDELINES DEFINITIONS

These guidelines are primarily focused at two major groups in the mobile ecosystem: Ad Providers and App Publishers. The following definitions provide context behind each of these groups.

- **App Publishers** – Includes the parties responsible for the development, publishing, and maintenance of mobile applications.

- **Ad Providers** – Primarily includes ad networks that are commonly embedded in mobile applications to manage ad delivery. Also includes mobile ad mediation layers, which manage the delivery of mobile advertisements across a number of distinct ad networks. This group also encompasses Ad Exchanges / Supply Side Platforms (SSPs) and Demand Side Platforms (DSPs) in cases where such groups collect, use, and retain device- or user-specific information.

GUIDELINES AT A GLANCE

While many of the specific guidelines and examples within this document have the potential to shift as user expectations evolve within the mobile context, the following principles should be adhered to wherever possible. Many of these recommendations have been particularly well articulated within the Obama Administration’s Consumer...
Data Privacy Framework, the EFF’s Mobile User Privacy Bill of Rights, and the joint CDT/FPF App Privacy Guidelines.

While this is not an exhaustive list of all the absolute requirements for App Publishers or Ad Providers, the items outlined below cover the most salient requirements to consider when handling personal information and exploring new forms of advertising.

The guidelines can be broken down into the following high-level categories:

1. **Provide Transparency and Clarity** to users about data collected, and present such information in a way that is readily accessible, easily understandable, and actionable by average users. The agreement to mandate specific privacy policy documentation for mobile apps is a start, but to be truly useful these privacy policies must be adapted for a mobile experience. In cases where Personal Information is collected (which can include name, phone number, email address, fine-grained location information, or more), simply providing detailed privacy policies may not be sufficient and requires gathering informed consent from users through the use of conspicuous, clear notification techniques prior to enabling data collection. This guideline has clear implications for App Publishers, but is especially important for Ad Providers, with whom mobile users rarely directly interact knowingly. When integrating with Ad Providers, App Publishers are responsible for ensuring that their users are properly notified of the privacy, security and usability implications that embedded third-party Ad Providers pose.

2. **Enable Individual Control** - Mobile users must be able to exercise control over what identifying data is collected by Ad Providers, and how it is used. This is tied closely to Transparency & Clarity, in that App Publishers must make it easy for users to understand what tools are available to them by communicating this from within the mobile app itself. In addition, mobile users should have the ability to withdraw consent from Ad Provider data collection and usage through accessible controls.

3. **Provide context and control when experimenting with new Ad Delivery Behavior.** Mobile Ad Providers have recently started to explore new methods of ad delivery, including delivering ads in the system notification bar (also known as “push” notification ads), placing new icons or shortcuts on the mobile desktop, and modifying browser settings such as bookmarks or the default homepage. When an ad is delivered outside the context of an individual application, mobile users have a right to know where the ad came from and how they can take action to control such behavior. More specifically:
   - Ad Providers experimenting with push notification ads must provide clear attribution to the source host application responsible.
   - Ad Providers that modify browser settings or add an icon to the mobile desktop must provide clear, conspicuous notice to users and gain explicit consent prior to doing so.

4. **Focused Data Collection** - Ad Providers should respect reasonable limits on the collection and retention of data collected from end user devices. The collection,
usage, and storage of data that can be used to uniquely identify a user or their
device must be performed in ways that are consistent with the context in which
users provide that data, and accompanied by methods of user notice that reflect
the relative privacy implications of such data. More specifically:

- Ad Providers should move away from using unchangeable device identifiers and
  should move towards using independent and/or temporal device identifiers that
  provide the same level of functionality with respect to targeted advertising.
- Ad Providers must not collect subscriber-specific identifiers such as MSI or
  MSISDN, unless the collection of such identifiers enables a demonstrable
  feature or service for the user (such as carrier-billing).

5. **Transport Security** - Device or user identifying data must be secured and
handled responsibly at all times by both App Publishers and Ad Providers.
Common security best practices such as transport layer encryption and forward
hashing should be a minimum standard. Mobile users have a right to expect
accountability from all members of the mobile ecosystem, including Ad Providers
and application developers. More specifically:

- When collecting unique device identifiers that are permanent and
  unchangeable by a user, Ad Providers MUST hash such identifiers using a
  generally accepted secure hashing algorithm and a unique salt.
- When collecting Personal Information such as email address or phone number,
  Ad Providers MUST transmit it securely using transport layer security (TLS / SSL).

**GUIDELINES PRIORITIZATION FRAMEWORK**

In this document, the key words “MUST”, “MUST NOT”, “ REQUIRED”, “SHALL”,
“SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT
RECOMMENDED”, “MAY”, and “OPTIONAL” are to be interpreted as described in
BCP 14, RFC 2119. They are used to provide an indication of the level of importance
of a requirement within the context of the guidelines in general. Overall there are two
main priority levels for these guidelines that should be stressed:

1. **Absolute Requirements** constitute the minimum level of behavior that App
Publishers and/or Ad Providers must follow to be in compliance with these
guidelines. Largely associated with the key words “MUST”, “MUST NOT”,
“ REQUIRED”, “SHALL”, and “SHALL NOT”.

2. **Recommended Requirements** constitute general best practices that App Publishers
and/or Ad Providers should follow wherever possible. Associated with the key words
“RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL”. 

[Image 25x30 to 156x62]
TARGET AUDIENCE FOR GUIDELINES

While this document does contain a selection of guidelines for mobile application developers, it is not intended to serve as a comprehensive reference for that audience, and there is a large set of guidelines that application publishers should consider, such as those provided by the Application Developers Alliance.

Due to the complex interdependencies between App Publishers and Ad Providers, a number of guidelines and best practices within this document are only applicable to specific parties. Wherever possible we have made an effort to make this distinction clear.

GUIDELINE DETAILS

1. Transparency and Clarity

First and foremost, App Publishers must provide straightforward information regarding data collection, use, disclosure and retention that is easily accessible from within their application. Such statements must also encompass the same information for any included analytics or advertising SDKs - including Ad Providers - and should be phrased in plain language understandable by the average consumer. Done properly, this type of disclosure should help mobile users understand what data is collected, who collects it, how it is collected, and how it is used (or shared).

Notice of Third-Party Data Collection

It’s common for App Publishers to integrate third-party code such as Ad Provider or ad analytics SDKs without providing any relevant context for how that code may affect user data collection and privacy. Some Ad Providers mandate the inclusion of specific copy within an application’s market description. While making the app deployment process easier for App Publishers (developers), this is often as ineffective as standard, long-form privacy policies, as the majority of mobile users do not take the time to read length app market descriptions. Data collection and usage that falls outside the reasonable expected context of an application - especially third-party data collection - should be signaled in an even more conspicuous manner that facilitates user understanding. In Focused Data Collection, we outline what data metrics are considered reasonable to collect from users, and what metrics require additional clarification for users and App Publishers alike.

Often, insufficient or inaccurate descriptions of third-party code within an application can be the result of an app publisher not fully understanding the implications of a given library or SDK. To this end, Ad Providers should provide a clear statement of data gathered and gating criteria (e.g. permissions required in the Android declarative permission model) with the goal of providing clarity to App Publishers regarding the additional
impact that including their code may have on the privacy posture of their applications. While it is incumbent on developers to include this information and in user disclosures of data collection and usage practices when integrating these SDKs into an application, Ad Providers should take a proactive approach to assisting developers in this endeavor.

**Notice of Ad Delivery Behavior**

In cases where third party libraries enable the delivery of non-standard or unexpected mobile ads (reference Ad Delivery Behavior for specific types of ads), App Publishers must follow similar practices of providing clear, conspicuous notice of such practices to users.

**Examples of Transparency and Clarity**

**Startapp Notice**

Startapp, a mobile Ad Provider that uses non-standard ad delivery methods to monetize applications through advertising, provides one of the best examples of transparent and clear notice to users about their practices to properly set user expectations. This includes mandating clear notification within an application’s description as well via a clear License Agreement on initial run of the app. Relevant information about non-standard ad delivery via desktop icons is presented above the fold for most device types, in clearly bulleted format.

![Startapp notice of non-standard monetization methods](FIGURE 1)
TRUSTe Privacy Policy Template

The mobile privacy policy template offered by TRUSTe provides a clear, digestible framework for presenting an accurate view of privacy implications for mobile users. It segments privacy concerns into information buckets that are most relevant for mobile users - including location services, tracking and ads, and security. In addition, it provides a clear mechanism to directly address the collection and use of identifying information.

FIGURE 2
TRUSTe mobile privacy policy example

Guidelines for Transparency and Clarity

Absolute Requirements

App Publishers (developers)

- App Publishers MUST provide clearly visible, understandable information regarding data collection, use, disclosure and retention that is easily accessible from a mobile context.
- App Publishers MUST include data collected by third parties such as Ad Providers within the scope of data collected by their application.
- App Publishers MUST keep such notice up-to-date with functional changes to external libraries or SDKs.
- In circumstances where third party libraries collect Personal Information (reference Focused Data Collection below) or deliver non-standard or unexpected advertisements (reference Ad Delivery Behavior), App Publishers MUST provided conspicuous notice and gain end user consent to such behavior prior to performing data collection.
- App Publishers creating applications directed at children MUST provide clear notice of information collection behaviors of any external third party libraries and MUST gain consent from parents before such behaviors are enabled.

Ad Providers

- Ad Providers MUST have clearly visible, understandable information regarding data collection, use, disclosure and retention that is easily accessible by consumers and App Publishers on their website.
Ad Providers MUST provide clear and proactive notifications to publishers on impact of changes to their SDKs.

**Recommended Best Practices**

**App Publishers**
- App Publishers SHOULD display information related to data collection by third parties or unexpected non-app publisher sources in a manner that makes this distinction clear and obvious.

**Ad Providers**
- Ad Providers SHOULD provide guidance to App Publishers around privacy implications of their capabilities, preferably in a format that makes it easy for App Publishers to consume and re-use, such as a privacy policy template.

**2. Enable Individual Control**

Beyond including straightforward, communicative information regarding data collection and use, it is essential that Ad Providers enable user controls over data collection and usage. Such controls should include - but not be limited to - the following:

- User-friendly controls to select targeted / interest-based advertising preferences, including the ability to opt-out of such targeting
- Mechanisms to withdraw consent to use personal or device specific information that has previously been collected

We understand that there may not be a way to effect a withdrawal of consent in the event that an Ad Provider does not retain exclusive control over data collected, or if the data collected cannot reasonably be associated with an individual.

Such controls should be made available to users through means and level of access that are roughly equivalent to those used to originally obtain or gain consent, preferably through straightforward, single-touch actions on a mobile form-factor.

**Relevant Example of Enabling Individual Control**

The TRUSTe Mobile Ads program is one of the most straightforward and fully-functional tools providing these user controls. Through the use of a consistent ‘AdChoices’ icon across partner advertisements, it provides a simple page where users can opt-out of collection and targeting from an individual network, or from all of TRUSTe’s partners. Those preferences are then remembered and enforced across all partners.
Guidelines for Enabling Individual Control

Absolute Requirements

Ad Providers

- Ad Providers MUST provide readily available opt-out mechanisms that allow users to control third party collection of Personal Information (reference Focused Data Collection below).
- Ad Providers MUST provide readily accessible materials that clearly outline the presence and effect of any available user data controls, including opt-in/out capabilities, as they relate to data collection, use, disclosure and retention, or non-standard ad delivery.
- Ad Providers MUST gain additional consent from users in instances where data is used for purposes that differ from those it was originally collected for.

Recommended Best Practices

Ad Providers

- Ad Providers SHOULD provide readily available mechanisms that allow users to control third party collection of device specific information.
- Ad Providers SHOULD respect the context of mobile and ensure that any control mechanisms they provide are fully accessible and configurable from mobile devices.
- Ad Providers SHOULD work towards the development of a single cross-network interface to allow users centralized management of their mobile ad preferences across a variety of Ad Providers.
- Ad Providers SHOULD begin to work towards developing a cross-provider persistent opt-out mechanism for both mobile web and mobile application-based advertising.

3. Ad Delivery Behavior

As the smartphone app model has evolved, advertising has continued to be a solid source of revenue for mobile developers seeking to offer free applications. For the vast majority of these applications, advertisements have been constrained to appear solely
within the confines of an individual application’s context. Recently, new and aggressive ad delivery techniques have emerged that include but are not limited to the following:

- Delivering ads within the standard device notification bar (also known as “push” notification ads)
- Inserting new icons or shortcuts on the mobile desktop
- Modifying browser settings like bookmarks or the default mobile homepage.

In addition, many Ad Providers are deploying new types of functionality linked to ad touch actions, including triggering of outgoing phone calls, text messages, or creation of calendar events.

These new tactics can often perform at better rates than traditional in-app display ads and can create new options for monetization. As a result they have increased in prevalence.

Application Coupling

The guidelines below distinguish between advertising access points that are coupled with a specific application, and access points that are not. This distinction has important consequences related to the expected user experience specifically related to the removal of such access points.

- Coupled Access Points use a specific hosting application to access the web. The removal of the application will directly influence ad serving or stop it completely. This category includes techniques such as notification ads.
- Decoupled Access Points do not rely on a specific hosting application to function properly. The removal of the application that created such access points will not affect ad serving. This category includes techniques such as icon ads or browser modifications.

Transparency

Each of these delivery techniques occurs outside the context of any individual application, making it difficult for a user to identify the specific application responsible or take action to permanently disable ad serving. As an example, the average user has no contextual basis for advertisements that are delivered through their notification bar apart from the content contained within the ad itself. We’ve seen that such lack of attribution increasingly results in user confusion and/or frustration.

If these methods of mobile advertising are to become broadly accepted within the mobile ecosystem, it is crucial that any advertising that is done outside of an app
contains significant additional methods of transparency for users.

- Coupled Access Points (such as push notification ads) are directly dependent on a host application to function. Such advertising methods must provide clear attribution to the host application to enable user controls.
- Decoupled Access Points (such as search shortcuts or icons) are independent of a host application. As such, it is essential for such advertising methods to provide clear opportunities for informed consent to users upon application installation and runtime. Providing clear instructions on how to remove decoupled access points is also important.

**User Controls**

Done right, transparency provides a user with a clearly defined set of actions to take if and when they wish to remove any specific advertising access point. While simply removing an application or advertising access point is one option for users, another option is to control delivery behavior through specific settings or controls.

**Guidelines for Ad Delivery Behavior**

**Absolute Requirements**

**Ad Providers**

- Advertisements delivered outside the context of an individual application via coupled access points MUST provide clear attribution to the host application. It is incumbent upon Ad Providers to work closely with its app publishing partners to enable conspicuous notice to users, gain appropriate consent, and provide attribution in such cases.
- Ad Providers serving advertisements delivered outside the context of an individual application via de-coupled access points MUST provide clear indications of such behavior and gain informed consent from users prior to ad delivery.
- Ad behavior that modifies device settings or desktop MUST be clearly communicated and strictly opt-in.
- Ad Providers that deliver advertisements outside the context of an individual application MUST provide an opt-in / opt-out mechanism for mobile users that is accessible from a mobile context.
- Ad Providers MUST ensure that advertisements that direct to out of band processes (such as touch-to-call or touch-to-sms ads) have clear notice of their behavior and require affirmative user action before the resulting process occurs (e.g. modal confirmation dialog before phone call is placed).
- In instances where opt-out mechanisms cannot automatically remove advertising
Recommended Best Practices

App Publishers

- App Publishers integrating with Ad Providers that deliver advertisements outside the context of an individual application SHOULD provide advertisement opt-in/opt-out mechanisms that are accessible from the app itself.

Ad Providers

- Ad Providers that deliver advertisements outside the context of an individual application SHOULD provide an option for users to stop receiving advertisements that is independent of the hosted application.
- Ad Providers SHOULD ensure that advertisements that direct to out of band processes (such as placing phone calls or sending SMS) do so through clear, individual opt-in consent each time a user clicks them. While it is reasonable for such consent to be applied across an individual application as a one-time acceptance, Ad Providers SHOULD NOT apply such consent across application contexts.

4. Focused Data Collection

Because user data is more valuable - it allows advertisers to serve targeted ads for potentially greater monetization opportunities - identifying unique users is core to the way Ad Providers operate in general.

Device Identifiers

To-date, one of the most common way to uniquely identify devices for targeted serving of mobile advertisements has been to use actual device identifiers such as the UDID, IMEI, or MAC Address, depending on the platform in question. While this commonplace practice has typically been viewed as acceptable, there are a number of concerns with this approach:

- Hardware Inconsistencies: WiFi-only devices such as tablets often do not have telephony hardware, and not all telephony devices have WiFi;
- Persistence: These identifiers persist across data wipes and factory resets and are tied to specific hardware
As a result we recommend that Ad Providers move away from using hardware-specific device identifiers and move towards using independent and/or temporal device identifiers that provide the same level of functionality with respect to targeted advertising.

The following lays out general guidelines for Ad Providers with respect to the most common device identifiers:

<table>
<thead>
<tr>
<th>IDENTIFIER</th>
<th>DESCRIPTION</th>
<th>CURRENT AD PROVIDER USAGE</th>
<th>USAGE GUIDELINES FOR AD PROVIDERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Mobile Equipment Identity (IMEI)</td>
<td>Globally unique identifier of a device. Device hardware-specific; user cannot clear or change IMEI.</td>
<td>Commonly used for consistent device identification.</td>
<td>SHOULD NOT be collected for advertising purposes; If collected, MUST be forward hashed to preserve user privacy.</td>
</tr>
<tr>
<td>Unique Device Identifier (UDID)</td>
<td>An alphanumeric string unique to each iOS device (iPhone, iPad). Device hardware-specific; user cannot clear or change UDID.</td>
<td>The most commonly used identifier for consistent device identification on iOS.</td>
<td>SHOULD NOT be collected for advertising purposes; As of iOS 5, MUST be accompanied by proactive opt-in/out notice.</td>
</tr>
<tr>
<td>Media Access Control (MAC) Address</td>
<td>Unique identifier assigned to a network interface for communication on the physical network. Device hardware-specific; user cannot clear or change MAC Address.</td>
<td>Occasionally collected for consistent device identification.</td>
<td>SHOULD NOT be collected for advertising purposes; If collected, MUST be forward hashed to preserve user privacy.</td>
</tr>
<tr>
<td>Android_ID</td>
<td>Unique to Android devices, a 64-bit identifier generated and stored when a device first boots. Impermanent - changes on device factory reset.</td>
<td>The most commonly used identifier for consistent device identification on Android.</td>
<td>MAY be collected for advertising purposes; If collected, SHOULD be forward hashed to enhance user privacy.</td>
</tr>
<tr>
<td>International Mobile Subscriber Identity (IMSI)</td>
<td>Globally unique identifier of a mobile subscriber. SIM-card specific; tied to an individual subscriber account.</td>
<td>Occasionally collected for subscriber targeting purposes.</td>
<td>MUST NOT be collected for advertising purposes; Reference specific guidelines for exception cases for collection.</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Globally unique identifier of a mobile subscriber. Simply put, it is the telephone number to an individual SIM card. SIM-card specific; tied to an individual subscriber account.</td>
<td>Infrequently collected for subscriber targeting purposes.</td>
<td>MUST NOT be collected for advertising purposes; Reference specific guidelines for exception cases for collection.</td>
</tr>
</tbody>
</table>
In place of hardware- or subscriber-specific identifiers such as those listed above, we strongly encourage Ad Providers to use a substitute metric that provides the same targeting functionality while preserving user privacy. The number of options available has expanded recently as Apple has begun to enforce its policy regarding collection of UDID, and now includes:

<table>
<thead>
<tr>
<th>IDENTIFIER FRAMEWORK</th>
<th>EXAMPLE(S)</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pasteboard Conversion Tracking</td>
<td>OpenUDID</td>
<td>Currently specific to iOS, Establishes independent device identifier persisted across apps through use of 'cut / paste board' mechanism. Some solutions (SecureUDID) provide option for global user opt-out of collection across any applications / services that use it.</td>
</tr>
<tr>
<td>Hashed MAC Address</td>
<td>ODIN</td>
<td>Generates ID numbers from the device MAC Address, establishing a single device identifier much as OpenUDID or the original UDID. Does not provide an option for end users to change or clear identifier.</td>
</tr>
<tr>
<td>Browser Redirects</td>
<td>AD-X</td>
<td>Consistent with online cookie-based framework, this method launches the device browser on click / conversion events to enable 1st party cookies. Works across apps and mobile web. Leverages current mechanisms to provide option for users to clear identifier(s) by clearing browser cookies.</td>
</tr>
<tr>
<td>Device Fingerprinting</td>
<td>Various</td>
<td>Builds a unique profile of a user based on various handset values, including OS version, timestamps, etc. Does not provide an option for end users to change or clear identifier.</td>
</tr>
</tbody>
</table>

In addition, there are indications that Apple may release its own identifier to be used for anonymous targeted advertising.

Many of these efforts to develop an industry-standard replacement for UDID are currently in flux, and we expect there to be significant change in the near-term as App Publishers and Ad Providers determine what practices are acceptable and/or preferred across various platforms. There are, however, clear advantages of several frameworks that have begun to emerge, and we currently recommend adopting a standard that incorporates features that improve the privacy of users, including:

- Provide users the ability to clear or change their specific identifier
- In cases where an identifier is tied to specific hardware and unchangeable, provide clear notice to users and opt-in/out capability

Personal Information

In contrast to Device Identifiers, Personal Information is data about an individual user that has the potential to be used for ad targeting. This information should not be collected by App Publishers or Ad Providers unless it is knowingly supplied by the user through means such as form submission, or after explicit consent is obtained from the user through an opt-in process. If and when user consent has been given to gather this information, it
is especially important that it be securely transmitted and stored - reference Transport Security. Personal information includes but is not limited to the following:

- Name
- Phone number
- Email address
- Demographic data
- Contacts or other social relationship information
- Browser history or bookmarks

**Location**

Location information is unique amongst personal information metrics for a number of reasons:

- **Granularity** – Location can be collected at levels of granularity that are not personally identifying for an individual
- **Behavioral Prediction** – When collected over longer periods of time, location information can be used to predict future behavior and location that is consistent with the granularity of data collected.

Each of these characteristics necessitates additional levels of consent in particular instances of location data collection.

The above guidelines cover the collection of personal information for the purposes of Ad Provider based reporting and targeting. In instances where this data is collected to enable customer-facing application features (i.e. location information collected for the purposes of displaying location to contacts or friends), it’s nevertheless important for App Publishers to clearly state such practices through best practices of Transparency and Clarity.

**Guidelines for Focused Data Collection**

Reference Device Identifier usage guidelines above in addition to the requirements below.

**Absolute Requirements**

**Ad Providers**

Ad Providers MUST NOT collect device identifiers that allow for the unique identification of individual subscriber(s) such as IMSI or MSISDN, unless the collection of such identifiers enables a demonstrable user-facing feature or service (e.g. Mobile Network Operator integration that requires subscriber data). In such exception cases, Ad Providers MUST provide clear, conspicuous notice of identifier collection that is consistent with Transparency and Clarity guidelines.
o When collecting unique device identifiers that are permanent and unchangeable by a user, Ad Providers MUST hash such identifiers using a generally accepted secure hashing algorithm and a unique salt.

o When collecting Personal Information (as defined above), or fine-grained location information, Ad Providers MUST provide conspicuous notice and gain end user consent to such behavior prior to performing data collection.

o When collecting Personal Information (as defined above), Ad Providers MUST transmit such data using secure methods (reference Transport Security).

o Ad Providers MUST provide clear, conspicuous notice to users when retaining location information beyond the timeframe reasonable for immediate ad delivery.

Recommended Best Practices

Ad Providers

- Ad Providers SHOULD NOT rely on hardware-specific unique values such as IMEI, UDID, or MAC Address for use in targeted advertising.
- Ad Providers SHOULD NOT collect unique device identifiers used for targeted advertising without notifying users of such behavior and providing a readily available opt-out option to users.

5. Transport Security

While proper communication is a first step in building behavioral transparency into the mobile ad industry, messaging does not address the security or privacy of that data. Properly maintaining user privacy while collecting such sensitive and specific information is highly dependent on the methods used for collection, transport and retention of the data itself. Improper handling of such information can result in inadvertent disclosure, embarrassment or reputational harm, and financial damage through lawsuits or user loss. Such consequences have the potential to affect both App Publishers and Ad Providers. Covering the full breadth of data security best practices is best suited for its own set of guidelines. As such we’ve chosen to focus here on guidelines specific to the transport of personal or device specific data.

Forward Hashing

It’s often the case that specific data metrics - such as UDID or IMEI - provide value to Ad Providers or App Publishers merely through their uniqueness. For data metrics such as these that carry with them privacy concerns, using ‘one way’ cryptographic hash functions such as SHA-1 or MD5 can preserve the uniqueness of a metric while protecting user privacy by obfuscating the original value. It is critical that Ad Providers use a unique salt when using any such hash functions in order to defeat specific types of attack such as lookup or rainbow tables. In addition, Ad Providers should follow the guidelines put forth in Focused Data Collection with respect to handling such device identifiers.
TLS / SSL

Beyond providing proper notice to users of information collection of ad delivery techniques, one of the biggest current issues with Ad Providers is a lack of basic transport security to protect Personal Information collect. This finding applies to Ad Providers large and small and includes not just those that collect large amounts of personal information, but also those that collect only a single identifier such as the IMEI.

Guidelines for Transport Security

Absolute Requirements

Ad Providers

- Ad Providers MUST forward hash device identifying information using a generally accepted secure hashing algorithm and a unique before collecting it from the device for the purposes of delivering targeted advertising.
- When collecting Personal Information (as defined in Focused Data Collection), Ad Providers MUST transmit it securely using transport layer security (TLS / SSL).

Recommended Best Practices

Ad Providers

- Ad Providers that disclose identifying data to third parties SHOULD at a minimum ensure the recipients are under enforceable contractual obligations to adhere to appropriate data handling guidelines, including those provided in this document.

CONCLUSIONS & NEXT STEPS

It has been clearly demonstrated that users have an underlying expectation of reasonable standards for mobile privacy and security best practices. These guidelines are meant to provide a reference point for all participants in the mobile ecosystem - from Ad Providers to App Publishers to end users - to assess proper and improper behavior:

- Absolute Requirements should be used as a behavioral baseline of minimally acceptable practices. Ad Providers that are not in compliance with this set of guidelines may be assessed as privacy infringers or adware.
- Recommended Best Practices should be viewed as best case behaviors. Ad Providers that incorporate these guidelines should be viewed as industry leaders.

The mobile advertising ecosystem consists of complex relationships between Ad Providers, App Publishers, and end users. Due to this complexity, it’s often difficult for consumers to grasp the degree to which their information has been collected and shared. Industry regulation, which increasingly becomes a possibility as new aggressive
forms of ad delivery and information collection are explored, is something that can only be avoided with full information disclosure to end users. It is the collective responsibility of Ad Providers and application developers to ensure that users are fully informed and empowered to control practices that capture information that is specific to their device or personal life. Two important aspects of that shared responsibility are:

- App Publishers should be mindful of what Ad Providers they integrate into their applications; optimizing monetary return should not be the only consideration; App Publishers should know what information about their users is collected and how that information is handled.
- Ad Providers should make the app integration decision easy for App Publishers by making their practices around user security and privacy as upfront as possible. This includes development of comprehensive, readable privacy policies and related FAQs.

Living Specification

As the mobile industry continues to evolve at an ever-increasing pace, we expect that these guidelines will continue to change along with it. In this regard, these guidelines should be interpreted as a living document that has the potential to change significantly as mobile privacy and security best practices evolve.