Mobile Privacy Demystified

Tracking and privacy – myths, myth busting and solutions

It seems everybody is talking more and more about mobile advertising, and in particular Tracking and Privacy these days. It's more than just hot air – a few companies ended up in the spotlight and in serious trouble over the past year due to violation of these very topics.

As a result the industry has been scrambling somewhat and everybody is jumping on to the topic, often without completely understanding what it really means.

Both terms have very broad meaning in the online and mobile advertising markets and it always pays well to clarify exactly what is being discussed before jumping to conclusions.

Tracking and Privacy can mean different things to different groups. Read on to find out about the many pieces which make up the puzzle.

Impression cookies

When talking about tracking in digital advertising, one may refer to recording of anonymous page and site visit user statistics in combination with ads viewed on said sites and pages. Such tracking involves the placing of a cookie onto the user's device browser, be it a desktop machine, iPad or mobile phone, to uniquely identify them on repeat visits to the server.

A cookie is a standard mechanism for storing data on the user's browser. It has been built into all browsers pretty much since their arrival.

Cookies were mainly invented to store things like sessions IDs and logins, so you would not need to keep typing your user name and password in again and again. For example, without cookies, if you were browsing the eBay site – every time you clicked a link to a new page, you would need to re-enter your login details, which of course would make it almost unusable.

Without cookies, the world of web would be a bit like the "50 first dates" movie, or, for the art house movie aficionados – "Memento".

Since then, the advertising industry quickly adopted the humble cookie as a method to track audiences and without it a lot of the online advertising would not exist in the form that it does today.

The various tracking cookies are specific and contextual to the ad exchange and media buyer platforms. I.e. one exchange or media buyer cannot just use another's cookie – without them agreeing first to share this data.

To clarify a few terms, such as ad exchange and media buyer, see below.

An ad exchange is a trading place for digital media. It's just like a stock exchange except the commodity is banner space on sites and in apps. All space is sold on demand, i.e. the trade occurs when somebody starts to load a page where an ad could be shown. There are many exchanges out there, such as Google AdX, Admeld (now part of Google), Nexage and Smaato, to name a few.

A media buyer platform is a system built to automatically, or as it's otherwise known – programmatically – buy from these exchanges. A Demand Side Platform (or DSP) is such a tool. There are several on the market and for mobile specifically there is currently only one, mobile dedicated, self service DSP – StrikeAd Fusion. StrikeAd Fusion is also integrated into all the aforementioned exchanges.

Other DSPs, all mobile or with some mobile capability, include Google's Turn, MediaMath and DataXu.

Coming back to cookies and their ownership by the exchange or SSP: for example, a Google DoubleClick cookie cannot be used by Yahoo Right Media and vice versa.

Some exchanges may also make a note of which sites or type of sites the user visits to show them ads, which are more relevant to them. Unfortunately, this process can freak out some consumers, as they don't understand how it happens and think big brother is watching their every move.

For the record, a cookie is not some Trojan horse designed to suck all of the users' data such as credit card and pin numbers, passport number and so on. A cookie is just an anonymous unique user ID by which the advertisers' servers identify the device. It's more like a hotel door card – it just lets you into the hotel and your room and tells the hotel when you came in and out but without exposing your name and many other details.

From this ID the ad exchange and advertiser do not know who the person is. They just know it is the same person that saw the ad a few minutes ago.

The major positive effect of ad matching to audience is seeing ads for products the said users may actually be interested in, rather than something random and sometimes annoying.

The main point here is that a cookie does not provide the advertiser with a pointer to the real person, their name and address. Such data is known as PII or Personally Identifiable Information and as long as you're not handling it – there are no legal or other issues to worry about.

PII, privacy and everything else – some background

There are a number of key principles that one needs to understand when dealing with users' data.

The first one is **PII or Personally Identifiable Information**. PII is essentially any kind of data that can be tracked back to the person.

PII consists of any information that can, directly or indirectly:

1. Identify an individual, including but not limited to name, address, IP address, SSN and/or other assigned identifier, or a combination of unique or non-unique identifying elements associated with a particular individual or that can be reasonably associated with a particular individual, or
2. Permit a set of behaviours or actions to be consistently associated with a particular individual or computer user, even if the individual or computer user is never identified by name or other individual identifier. Any set of actions and behaviours of an

individual, if those actions create a uniquely identified being, is considered PII because the associated behavioural record can have tracking and/or targeting consequences.

Non-Personally Identifiable information (Non-PII) is:

1. Aggregated data not associated with any individual or any individual identifier, or
2. Any individual level data that is not PII.

An anonymous user ID stored in a cookie is non-PII, since from that ID it's impossible to work out who the real person behind it is. It's like wearing a mask and a picture-less ID badge every time you go into a building – the doors will open for you but the guard will never know who you really are.

The other key principle one needs to be aware of in privacy is disclosure and opt out.

Legislations then split into two streams – EU and USA.

Cookies and HTML5 database

There are two ways to store the user ID on the mobile device. The first is through using the Cookie we've talked about earlier.

On iOS, i.e. iPhones, iPads and the iPod Touch, however, it is not possible to set cookies which are not from the same domain as the domain of the page you're on. This is covered in detail in the StrikeAd App Tracking without UDID White Paper about download attribution, so we won't go into it again here.

To get around this limitation, another way to set data on the client side is to save it using a function of JavaScript and HTML5 (if the browser supports it), which provision client side (i.e. in the browser) data storage. This does involve executing some JavaScript in the user's browser, however – not necessarily a big issue.

In other words, a server can save data it can read later from the browser by executing more code on the HTML page.

Some sites use it to store data which will be accessed again and which may be needed quickly or whilst the device is off line. For example, Google Web Mail does this and thus allows users to read emails they've downloaded previously without having to re-download them again and even if they're offline.

This same approach is now being used by some advertisers to store the said device and user IDs.

Fingerprinting

Another way to track user is to identify them from observed data, instead of tagging them. One such way is fingerprinting, or device profile based tracking.

The name that has stuck is pretty unfortunate as it sounds very "big brother" and has been getting some negative press. A more appropriate name would be “**Device Distinction**”. As in, trying to distinguish a unique device amongst many that look the same.

When a user visits a web site server, a number of properties that describe the device and browser are communicated to help format the web site right for the device. It could be screen size, colour capabilities, preferred language, browser versions (useful to avert bugs) and availability of plug-ins such as Flash, and ability to view certain types of audio and video.

The process of Device Distinction is based on using all sorts of properties from the information that comes to the advertising server from the users’ device to build a unique combination, which becomes the device identifier.

Again, there is no sinister process of recording deeply personal data about the user involved here, i.e. the swirls and curves of their fingerprint are not being secretly extracted and logged. Rather, generic and non-personal information is noted and used to form a profile.

Companies which are utilizing this method use properties such as the device time zone, country, device manufacturer name, model, OS, browser vendor and version, time locale, pre-set language and so on to build the combined device ID.

For example, one such profile may look like this:

“GMT; GB; Samsung, Galaxy Tab, Android, 4.0, Chrome 1.2; English”

As you can see, there are no surnames, passport numbers or anything else sinister.

It is a bit like using a combination of hair colour, height, weight, shoe size and so on to uniquely define a person. On their own the said properties are not unique, but put together, you will probably only find 1-2 people that match out of thousands. The principle is the same with the above mobile device properties.

In a way, fingerprinting is better than cookies as it does not store anything on the user’s device. This is great, especially since some devices don’t work well with cookies – but it is not as precise as a cookie.

It also has the added benefit of being compliant with the EU regulation, which does not allow storing of data on the client device but does not say anything about storing data about users on the server. Read more about the EU regulation further in the document.

What gets companies into trouble?

With all this technology explained, what is it actually that gets companies into trouble, get them sued and portrayed negatively in the press?

Typically, it is a lack of two processes within their tracking system(s):

- Disclosure
- Opt out or difficult to execute opt-out

Pretty much all the trouble in advertising around tracking has been to do with a lack of disclosure and opt out or doing something without providing either, e.g. handling PII data without disclosure or opt out.

The simple truth is – if you clearly tell the user what's going on and allow them to be excluded from the process – no laws are broken and the user, regulatory bodies and the government are happy.

We've all seen the little "i" icon in the corner of online ads.

When clicked, this icon takes the user to a page, where the whole ad preferences and matching, its intended use and benefits to the user are explained.

That's all you need to do for "disclosure".

On this page, the user is also allowed to opt out of the tracking by just clicking a big "don't track me any more" button. This sets the cookie on their device with a "do not track" flag and the next time the server reads the cookie, as soon as it sees the "don't track me" flag – it does not do any tracking.

See also further down information about the EU opt out directive.

Explicit Opt In – the end of an era?

All this is soon to change and users will be required to opt into cookie-tagging. EU is about to release a regulation requiring third parties to explicitly ask the user to allow the cookie to be set, as opposed to the above opt out.

Once this goes live, many sites and apps – or advertisers and agencies themselves – will have to facilitate this or the advertiser will not be able to carry out frequency capping or re-targeting any more.

There are a number of ways to go here – a header info block on sites, asking the user to allow this. A header block is extra information that a browser and server can use to pass invisible information to each other. For example, the browser passed to the server via the header block it's User Agent String, which contains the browser name, version etc.

The information then would be passed to the advertiser, who would set the cookie. If the "allow tracking" information was not sent, the advertiser would not set cookies.

With apps, a similar approach would be possible – when the app is first started, the user is asked if they are happy to opt into "ad choices" which will try and show them ads which are more suitable by remembering their preference.

If the user allows this, the publisher would pass the information to the advertiser, who can then track the user.

Legislations, law and industry regulations

It is important to understand that legislations are national, not global, and that different laws apply in different countries and compliance work therefore has to be tailored to respond to each one specifically.

EU legislation

Since 2003, anyone using cookies has been required to provide clear information about those cookies, according to legislation released at the time and a way for a person to opt out of such “tagging”. The rules were set out in the 2002/58/EC Regulations European Directive, which is concerned with the protection of privacy in the electronic communications sector.

In 2009 this Directive was amended by Directive 2009/136/EC. Under the revised Regulations the requirement is not just to provide clear information about the cookies and facilitate opt out but instead to obtain consent from users or subscribers to store a cookie on their device before the data is stored or a cookie is set.

The ICO (Information Commissioners Office) released a document detailing all the background, legal changes, impact on business and possible implementations to achieve compliance, which is hyper linked below. The document is very comprehensive and is a must read for anybody concerned with cookie legislations.

http://www.ico.gov.uk/%7E/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf

The new rules go into effect 26/05/2012 – a little less than 3 months left!

The regulation applies to pretty much any mechanism used to store data on the users’ local device – this includes LSOs or “Flash Cookies”, HTML5 data store (or database – now deprecated) and any future inventions that all do the same thing.

From May 26th onwards, anybody setting cookies which are not essential to the operation of the website (e.g. helping maintain a login) will need to ask the user to allow this to happen.

No more silent cookie setting.

Full 2003 “opt-out” legislation text is available at the below URL:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

The updated 2009/136/EC directive is at the URL below.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:en:HTML

The changes to the legislation mean that by May 25th 2012, the various EU Governments have to ensure that…

“…Those setting cookies must:

- ***Tell people that the cookies are there,***
- ***Explain what the cookies are doing, and***
- ***Obtain their consent to store a cookie on their device.****”*

The UK, for example, introduced the amendments on 25 May 2011 through The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

The full directive is available at the URL below:

http://www.legislation.gov.uk/uksi/2011/1208/contents/made

USA Legislation

There are no specific legislations on tracking specifically in the USA yet but the DAA (Digital Advertising Alliance) and the NAI (Network Advertising Initiative, URLs below) have released industry level recommendations and mandates.

http://www.aboutads.info/

http://www.networkadvertising.org

The mandates aim to help provide a safe working environment in the market and facilitate a solution which treats consumers fairly. The main aim and solution of said regulations are the mechanisms for disclose and opt out.

There are also some other existing legislations, however.

For example there is the Privacy Act of 1974, 5 U.S.C. § 552a (full citation URL below), which establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

http://www.justice.gov/opcl/privstat.htm

There is also the “Section 5 of the FTC Act”, which prohibits entities from engaging in unfair or deceptive acts or practices in interstate commerce.

http://www.law.cornell.edu/uscode/text/15/41

Another somewhat related legislation is the FTC Policy Statement on Deception, URL also listed below:

http://www.ftc.gov/bcp/policystmt/ad-decept.htm

Even more recently, after some news about major US companies were found to be potentially overriding user preferences and iOS limitations to serve targeted ads, the White House was prompted to draft a proposal on user privacy and security called the Consumer Privacy Bill of Rights. This bill currently has little to no support in Congress, but it does show that political awareness is rising.

Do Not Track initiative

A recent initiative, started by the W3C – the folks who invented the Internet standards and continue to evolve them – is the Do Not Track or DNT standard.

The DNT initiative defines a standard header block to be passed by the browser to the server. It is a way for a web client, e.g. a web browser, or an app, to declare to the server that it does not want to be tracked.

It's the best way for the user to tell the world they don't want to be tracked, as it then does not even require a cookie to be set by the various servers to do the same thing. So for those extra paranoid people it's like a "no unsolicited sales calls" sticker on the door, as opposed to having to mail back all the junk mail senders asking them not to do so any more.

This approach is Informational, as opposed to Blocking – like the cookie blocking mechanisms. In other words, the server has to honour the browser's request but can ignore it as there is nothing to stop it from doing so physically.

Even if the user or device is being identified using the fingerprinting method, which as I mentioned is not precise, with the DNT approach, as long as the server does not ignore the flag, the user will never be tracked.

The only problem is that for this DNT initiative to work, all browsers out there need to support the DNT initiative and provide the "turn DNT on" switch in the browser settings. Most desktop browsers now support the DNT on/off in settings – Mozilla FireFox v10, Apple Mac OS X Safari (Lion onwards) and Microsoft Internet Explorer v10. Google Chrome announced in February that it will also soon support the DNT header.

But only one mobile browser currently supports the DNT initiative – FireFox for Android. Safari for iOS and Google Chrome Mobile currently do not support DNT.

The DNT initiative website is at the URL below.

http://donottrack.us/

There is some independent information on DNT below.

http://en.wikipedia.org/wiki/Do_not_track_header

How to stay compliant – practical applications

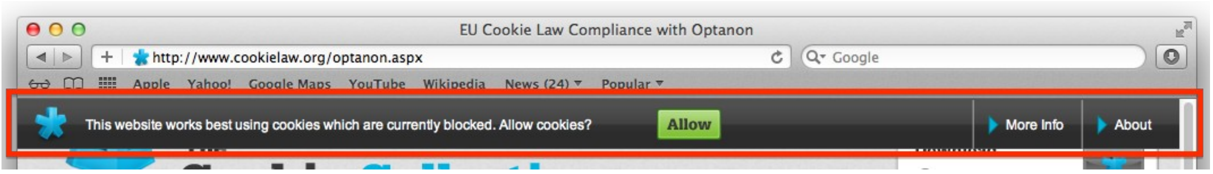
With all these regulations clear and explained, the conclusion is what to implement practically to ensure compliance. Compliance, just as the regulations, differ between countries.

For compliance in the European Union and the United Kingdom

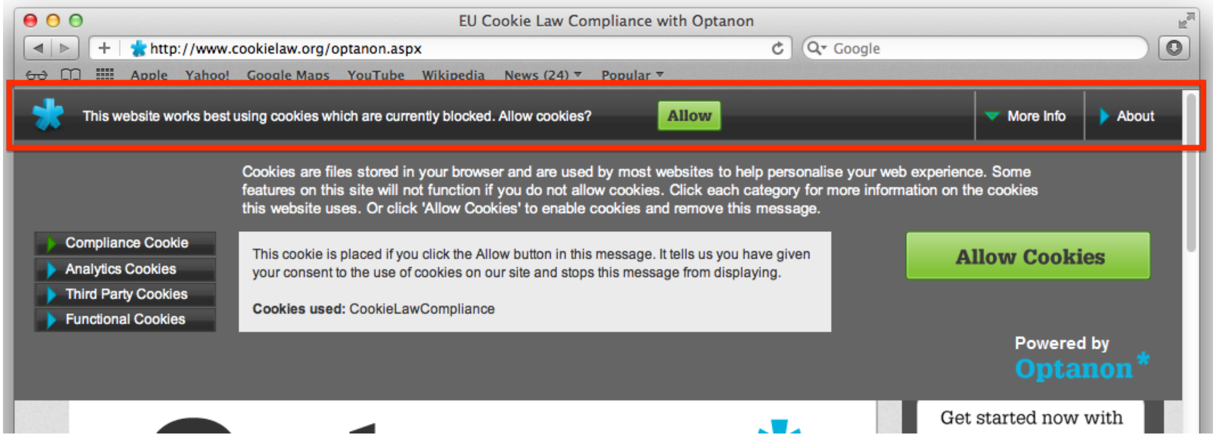
For the EU operations, the safest thing to do is provide users with a clear message upon entry onto the site or before a cookie needs to be set.

A simple way of doing this is by adding a thin "header" to the design and layout of the website, which would briefly outline the cookie setting attempt and provide a link to further, more detailed information about the cookie being set.

In the online world there are several suppliers providing such technology, for example Optanon.


EU Cookie Law Compliance with Optanon
http://www.cookielaw.org/optanon.aspx
Google
Apple Yahoo! Google Maps YouTube Wikipedia News (24) Popular
Allow
More Info
About

This website works best using cookies which are currently blocked. Allow cookies?



This website works best using cookies which are currently blocked. Allow cookies?

Cookies are files stored in your browser and are used by most websites to help personalise your web experience. Some features on this site will not function if you do not allow cookies. Click each category for more information on the cookies this website uses. Or click 'Allow Cookies' to enable cookies and remove this message.

This cookie is placed if you click the Allow button in this message. It tells us you have given your consent to the use of cookies on our site and stops this message from displaying.

Cookies used: CookieLawCompliance

This is quite easy to implement both in the on-line digital desktop world and in mobile.

In mobile, both web sites and applications would need to do this.

This is because is it not only mobile sites that have cookies or store local data about the user. Mobile apps also record such information and pass it to various servers, amongst them advertising ones. Some apps also synchronise their internal data and IDs to mobile web browser cookies. There are several companies on the market who do this to facilitate running of performance advertising campaigns across mobile web and in-app media.

This cookie synchronisation process is also covered in detail in the StrikeAd UDID-less tracking Whitepaper so we won't go into it here.

The cookie synchronisation process also further necessitates the cookie opt-in mechanism to be present in such situations.

There are two parties involved in the cookie setting and the requirement to obtain opt-in permission:

1. The web site or app that the user is viewing
2. The advertising server setting the 3rd party cookie

The web site or app owner does not need to ask permission from the user to store a cookie as long as the cookie is only stored for essential web site feature operation, such as shopping cart information and log in data.

This just leaves the advertising server.

One approach to obtain cookie setting permission here would be to pop-up a dialogue from the banner. However, this would not be very pretty so it's much better for the advertising server to work with the website publisher and to integrate the dialogue into the site design in a much nicer way.

The advertising server then just needs to pass the information about a user to the next site where the cookies are used, so that site knows that there is no need to ask this user to set a cookie since they've already given permission to do so.

This could be done by what's known as "cookie syncing" – a process of (usually) two-way sharing of cookie IDs so that the advertiser knows that site xyz.com user cookie ID 123 is the same as the advertiser's user cookie ID 789.

For compliance in the USA

In the United States, as described earlier, there are currently no legislations and only industry self-regulations exist.

The regulations require clear information about the user being 'cookied' or tagged and a straightforward opt out mechanism to be provided to that user.

To facilitate this, companies are best to take the currently common approach of the online digital desktop world of advertising, i.e. superimposition of the "i" icon in the corner of the ad and the icon also being a link to an information and opt out page.

There are currently a number of efforts under way in the mobile advertising industry to standardise the icon implementation and aggregate opt out pages, so that users can go to one aggregator's page to opt out of many cookies.

Is mobile different from online?

The short answer is – not really.

Mobile is just another way of accessing HTML pages on Internet servers, be it on a smaller device without a fixed cable.

Legislation, regulations and enforcement may not yet have focussed on the mobile advertising industry but it will with the pace at which the market is growing – and when it does, it is best to be ready.

This is clearly illustrated by the recent legal actions in the mobile world, which were linked to tracking, lack of disclosure and difficult opt out.

Conclusion

Hopefully you now have a good understanding of all the issues involved, technical and legal.

The key things to remember are:

- If setting cookies in the UK or EU – ask the user first!
- If doing so in the USA – show this clearly and allow the user to opt out

If you want to know more still, contact StrikeAd and we'd be happy to help!