Privacy-Conscious Marketing:

How iSIGN's PAN Solution Respects User Anonymity

iSIGN MEDIA CORP

© www.isignmedia.com

Enhance user privacy and you enhance your brand as well.

Today's consumers are more technically savvy than ever before. They are more cognizant of how technology works both for and against their interests,how it can be leveraged to accomplish any given goal, and also how it can be abused to create a negative outcome.

Nowhere is that made more clear than in the specific subject of how businesses track and utilize user data — and respect or disrespect user privacy. As the world has increasingly converged on IP-based services, those services have increasingly been leveraged not just to fulfill user requests, but, over time, to build a database of user information for marketing purposes. That data is, in many cases, fairly sensitive: user names, street addresses, phone numbers, social relationships, email, purchasing patterns, work history, income history, photographs, ad infinitum.

Exactly which information is collected, and how it is utilized for marketing purposes, differs from case to case. Some organizations use it responsibly. Others, driven by profit objectives, have been observed to act in an imprudent fashion, based on the premise that it is easier to ask forgiveness than permission.

Complicating this situation is the fact that government legislation on this subject has been slow to emerge — a reflection of the fact that society itself has not established everyday rules of thumb concerning what is and what is not acceptable. What's clear, however, is that organizations must find new ways to protect sensitive user information.

Failure to do so will likely result in significant brand damage.

Fighting Back: Taking Action Over Unwanted SMS Messagess

Over the past few years, a number of major lawsuits have demonstrated to advertisers that SMS spam can be very costly. A look at some cases that have helped pave the way for major change in consumer privacy:

- Simon & Schuster (2007) – Settled for $10 Million ($175 per phone number)
- Timberland Company (2008) – Settled for $7 Million ($150 per phone number)
- Burger King (2009) – Settled for $510,000 ($250 per phone number)
- Twentieth Century Fox (2010) – Settled for $16 Million ($200 per phone number)

Mobile: A marketing platform that can create new value — or subtract it

Perhaps the clearest example of this evolving phenomenon lies in the use of mobile phone data collected by communications service providers, mobile phone manufacturers, and social networking services.

In recent months, a number of scandals have demonstrated that users are unhappy to find that personal data they had considered private is, in fact, not private at all. It is instead shared among business partners, clients, and other groups, often for marketing purposes.

Facebook, for instance, owns the world's largest database of global user information, updated on a mass scale by millions of users every day in remarkable detail, often using mobile platforms. And Facebook has repeatedly revealed user data in ways its users never intended, in direct contradiction of both the Facebook privacy policy and users' privacy settings.

Similarly, Apple and Google, creators of the two most dominant smartphone platforms in the iPhone and Android respectively, have recently come under fire from the general public due to the discovery that users' geographical locations can be, and have been, tracked by mobile phones over time.

Public relations scandals of this type have the effect of diminishing the appeal of the smartphone in a broad sense. Instead of perceiving smartphones as a powerful, centralized portal to interact with the world via digital services, users now also increasingly perceive smartphones as a means by which they can be monitored and tracked in an almost Orwellian fashion.

This problem has been pronounced enough, and widely publicized in the media enough, that even legislators — historically slow to respond to technological shifts — have called hearings to interview corporate executives. Their purpose: to discover exactly what data businesses collect,what they do with that data, and why.

And the response has not always met the public's expectations. In one case, for instance, a smartphone manufacturer claimed that it was simply "a bug" that was responsible for collecting and storing data on user locations going back more than a year.
Exactly how much brand damage has accrued as a result may not be quantifiable, but it is certainly significant.

SPAM ALERT:

Unwanted SMS text becoming a big problem for consumers.

Consumers today are very active texters – over 52,082 SMS text messages are sent each second. But the growing number of these SMS messages are uninvited and unwanted spam. AdaptiveMobile reported blocking an average of **1.6 million unwanted SMS messages per month** – of which **60%** are **rogue advertising messages**. The FCC, responding to widespread consumer complaints, has taken action to curtail this abuse on the part of advertisers by enacting the CAN-SPAM Act in 2003. Intended to help curb spam, the act penalizes spammers and allows consumers to lodge formal complaints against offending parties.

© www.isignmedia.com

Respect for user privacy should be baked into solutions and services from the start — not bolted on afterwards.

The lesson for technology solution providers is clear: User privacy should be respected at all costs.

That means much more than just establishing clear privacy policies and consistently operating within those boundaries. It also means designing solutions and services that, from the start, make user privacy a high priority in the way they work.

The trend in the past has been that when in doubt, solution and service providers aggregate and analyze as much user data as they legally can. The trend going forward should be that when in doubt, solutions and services collect only the data they need to create user value or fulfill user service requests, and no more.

For marketing purposes, of course, this revised approach creates a bit of a dilemma.

Vendors do need some type of specific user information to best serve their clients and customers in a specific fashion. The only alternative is generic marketing — something much closer to junk mail than most users would like, yielding a poor outcome for both businesses and their customers.

The question, then, is: How can vendors fulfill specific user needs and interests, via targeted marketing, without compromising user privacy in any way?

iSIGN's PAN solution drives customized marketing campaigns while creating zero privacy complications

One excellent answer to that question: iSIGN's IMS (Interactive Marketing Solution) 3.1.

This leading solution serves as a privacy-conscious liaison between vendors and users — one that delivers targeted campaigns, yet also respects the privacy of sensitive user data at every stage.

To accomplish this, **IMS 3.1** leverages the concept of the **Personal Area Network (PAN)** based on the Bluetooth broadcasting standard. Once deployed on site at a retail presence, the patent pending **IMS 3.1** solution detects, and communicates with, all Bluetooth-capable mobile phones that come within its limited range (from three to three hundred feet).

An initial inquiry is transmitted to the phone — such as "Would you like to know more about the following special offer?" — and, if answered affirmatively by the user, an appropriate marketing campaign is then transmitted.

That campaign, in turn, could be very simple or very complex depending on the vendors' marketing goals and the users' attention span and interest level. It could be as trivial as a coupon; or it could be,

something more like an immersive game designed to engage or educate users at a deeper level.

Regardless of campaign specifics, however, sensitive user data is never harvested from a phone, never transmitted over the air, never stored, never analyzed, and never correlated with other data pools for marketing purposes.

This is because **IMS 3.1** uses no human identifier, such as a name or phone number. Instead, it uses only hardware information associated with each particular phone.

Despite this preservation of consumer anonymity, however, **IMS 3.1** does allow vendors to develop, over time, a fairly comprehensive and detailed profile of user trends and audience interests on a large scale.

It also allows vendors to create and deliver pinpoint marketing that corresponds to specific locations — for instance, marketing campaigns that involve electronics products, and are sent to user phones if and only if that user is in the Home Electronics section of a department store.

This design means that users get tailored marketing that aligns closely to their interests — marketing that actually creates new value for them by giving them information they are likely to find useful. It also means there is no possibility that the privacy of their sensitive data won't be respected, because sensitive data is never collected in the first place.

iSIGN's solution is, with respect to user privacy, both proactive and end-to-end — addressing not just which data is collected, but the complete lifecycle of that data. Simultaneously, it supports vendor marketing goals and yields a superior business outcome and competitive distinction for them.

PERSONAL AREA NETWORK

Complete preservation of user anonymity at every stage, of every transaction, in every campaign

To illustrate just how **IMS 3.1** delivers these impressive benefits, let's walk through the specifics of what it does and does not do.

The first step taken by the solution is to collect a MAC (Media Access Control) interface address from the phone. This is the key identifier used in all IMS records — not the user's name, phone number, or any other sensitive information. Additional hardware information collected is the phone's make and model.

The next step is to transmit a campaign query and track the user's response (whether negative, positive, or a time-out due to no response). Naturally, to establish the success of different marketing campaigns, certain specifics about the campaign are recorded. Among others, these include the campaign title, the **personal area network** (**PAN**) in which the transaction took place, the user's dwell time inside that **PAN**, and user movement within the **PAN**.

Again, because there is no sensitive information included in any of these categories, user privacy is continually preserved.

If campaigns generate a positive response to the initial query, more information is then collected. A coupon might be redeemed or rejected; that redemption is recorded. Users might respond favorably to being invited to participate in loyalty programs and if so, that information will be recorded as well. Some vendors offer loyalty points to users who remain inside the retail space for extended periods of time, redeemable as discounts. If so, these points will aggregate in the IMS profile associated with each phone's MAC address.

At no time, however, is sensitive user data collected. Only two classes of data ever are: information pertaining to the phone itself, and anonymous user responses to different marketing campaigns.

Even in the case of campaign data, the focus in **IMS 3.1** is not to track individual behavior, but instead to discover and analyze crowd trends. What vendors need to know to create more successful marketing, as a general rule, is not the fine detail, but the broad brushstrokes: mass patterns that clearly establish which campaigns are more successful, which services are more in demand, and which products elicit more interest. This trending information is exactly what **IMS 3.1** delivers.

User privacy spans the full lifecycle of user data

Additional respect for user privacy is evident in the process by which data is transmitted and stored. Consider that no sensitive data moves across a vendor's **PAN**; this also means no sensitive user data is sent to, or hosted by **iSIGN** itself. At every stage in the data lifecycle, from initial acquisition to trend analysis and the creation of new campaigns, there is zero opportunity for user privacy to be abused because no specific user identifiers are ever harvested.

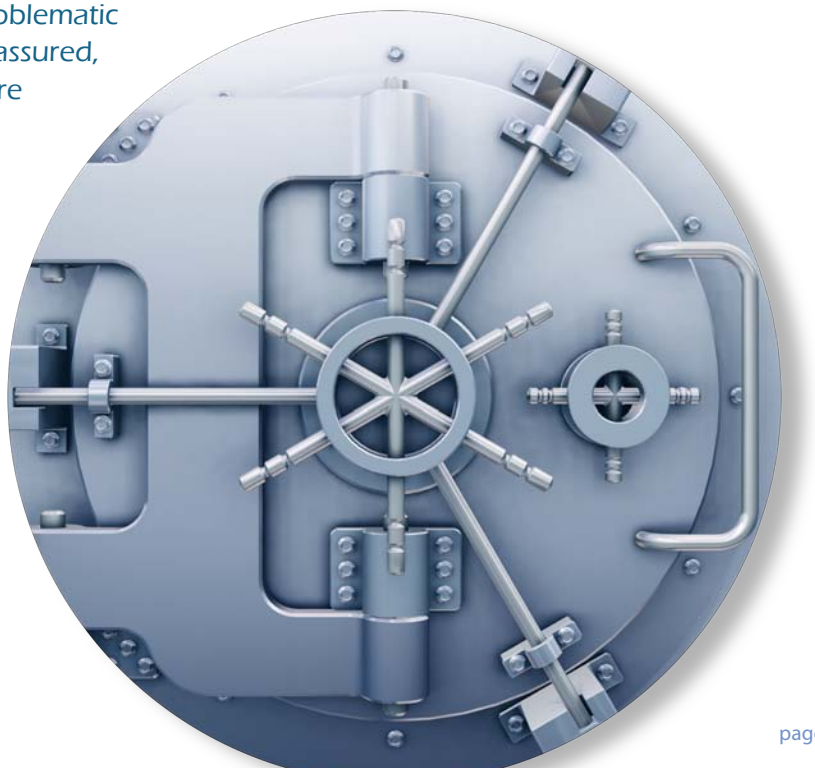
Furthermore, data is never shared between defined iSIGN customers. It is, instead, isolated, specifically to eliminate any possibility of cross-user sharing and a subsequent breach of privacy.

Additionally, user data is encrypted in different ways at different times. Besides being encrypted in transit over the Internet and on **iSIGN** servers, using the same 128-bit standards used by banks and healthcare providers, data is also (given successful pairing) encrypted in the initial Bluetooth transmissions between mobile phones and vendors.

What kind of security and privacy track record has this system created over time?

iSIGN has never experienced a security breach of any kind. There is not a single instance of user data being seen by unauthorized eyes, shared in an unexpected fashion, or leveraged to create any sort of unwanted outcome for **iSIGN** clients.

Instead, **iSIGN's IMS 3.1** solution simply delivers the intended value — tailored marketing that suits user needs — while generating no privacy-problematic side effects. User anonymity is assured, and yet vendors can learn more about what customers want and do not want, and provide increasingly better service to those customers over time.



iSIGN IMS 3.1: Get tremendous ROI and brand protection, all with comprehensive user anonymity

For proof of concept, as well as a specific example of the kind of value both consumers and vendors can achieve via **iSIGN's** solution, consider the following scenario:

A retail chain wants to drive up user awareness of new goods or services at a particular location. Toward that end, it deploys **IMS 3.1** to communicate with customers with Bluetooth-capable phones inside a three-hundred foot radius of the retail presence.

The odds those customers will be interested in such marketing campaigns is fairly high, given their geographic proximity — certainly much higher than it would be via any more traditional approach, such as bulk mail. And as a result, campaign redemption is typically a full order of magnitude higher for the vendor than it could reasonably expect via bulk mail.

Return on investment is relatively straightforward to establish, because the vendor can easily track both the ongoing costs and the business outcomes of IMS campaigns.

Deployment outcomes will naturally vary from case to case, but the following numbers illustrate the possibilities:

Monthly cost: $150/month.
Phones identified per month: 150,000
Redemption of marketing campaigns sent to those phones: 10%
Average revenue yielded per redemption: $50
Total monthly revenue generated via IMS campaigns: $750,000

Compare the cost ($150/month) to the revenue generated ($750K/month) in this scenario, and you begin to see just what kind of return on investment the **iSIGN** solution is capable of generating.

And because it comprehensively respects user privacy, **IMS 3.1** also generates impressive return on investment of a different kind: brand preservation and development.

Instead of having to address and resolve privacy scandals, **iSIGN** clients can focus on business goals and customer satisfaction.

Instead of having to develop and deploy new technologies and processes to meet evolving user privacy expectations, **iSIGN** clients can continue to leverage a trusted, proven solution with a perfect security record. There is simply no chance of a privacy breach because sensitive data is never harvested in the first place.

And instead of having to worry that their information will be harvested, shared, and utilized in ways unforeseeable to them, consumers can learn more about the products and services that interest them the most.

In this way, both the business and its customers benefit from a superior outcome over time. So, far from the business' brand being damaged, instead, it has been enhanced - the ultimate goal of all marketing.

Contact info:

For more information, please contact Alex Romanov of **iSIGN Media** at **+1.905.780.6200,** or email him at **alex@isignmedia.com.** For media enquiries, please contact Vanessa Horwell at **+1.305.749.5342 x232,** or at **vanessa@thinkinkpr.com**.

About iSIGN MEDIA:

Attract. Transact. Measure.
Best-in-class proximity marketing solutions from a proven leader

iSIGN Media stands out as a pioneer and industry leader among proximity marketing providers today. **iSIGN's** patent-pending solution empowers retailers to deliver content and offers to consumers at precisely the right place and the right time – ultimately resulting in targeted, accountable and measurable advertising.

Founded in 2006, **iSIGN** was one of the first to market with a Bluetooth™-based solution for a range of up to 300 feet, providing superior performance, and a superior customer experience. **iSIGN** offers one of the most flexible, scalable proximity marketing platforms, capable of supporting a rich array of different content types, including bandwidth-intensive video, as well as most media players and engines.

The **iSIGN** IMS technology allows retailers to create geographically-specific marketing campaigns that encourage increased consumer engagement. **iSIGN's** solution delivers content directly to consumers' cell phones while they are within a 300-foot radius or personal area network (PAN). Providing contextually relevant offers to consumers at the ideal time and place, the solution helps marketers drive consumer action through interactive, creative and unique marketing campaigns.

iSIGN's solution respects user privacy via opt-in functionality, and it doesn't collect or require personal information such as cell phone numbers or customer names. Information is instead associated with a unique technical identifier linked to the particular mobile device, and anonymously analyzed for subsequent business and marketing research purposes. This translates into customer peace of mind, and gives retailers the power to understand their customers' needs and interests in unprecedented detail.

Directly impacting advertisers' anticipated ROI and bottom line is the fact that **iSIGN's** expected total cost of ownership (TCO) is among the lowest in the industry. In fact, according to recent studies, it is the least expensive of all proximity marketing solutions currently on the market.

With **iSIGN's** solution, delivering targeted, rich marketing campaigns to customers involves less business risk and ongoing investment than ever before – all while yielding dramatically improved positive response levels.

iSIGN MEDIA CORP

PAN PERSONAL AREA NETWORK

www.isignmedia.com