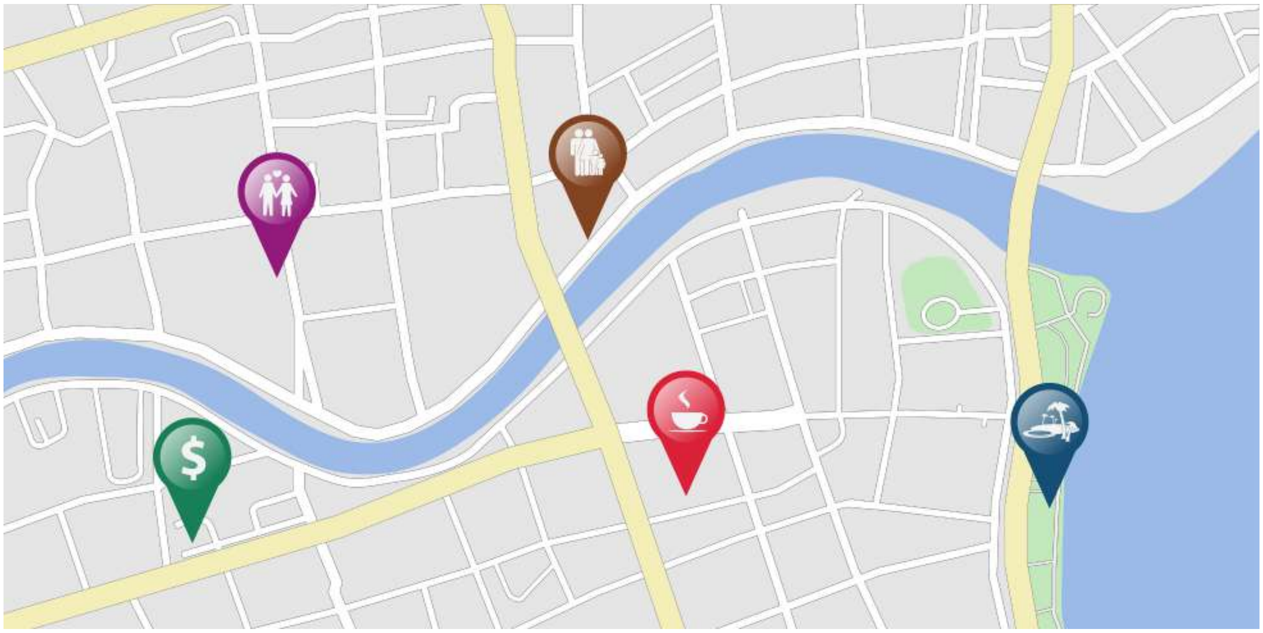
SOPHATAR
Personalized Displays that Know You!

PRESENTS



PROXIMITY MARKETING

DONE RIGHT: *WITH CUSTOMER OPT-IN*

INTRODUCTION

"To compete with online, brick & mortar retailers are to adopt personalization strategies just as websites do."

This statement, meanwhile a platitude, has been uttered by about every retail consultant by now. And of course it's true. It's just not so obvious in 2020 how to gather the data that allows you to do this in an environment that has become gradually more privacy-conscious over the past 24 months.

This whitepaper presents some of the proximity marketing methods used originally and why they have failed or at least are seeing increasing backlash both from a technical and regulatory perspective.

We'll then provide some possible solutions to, in an ethical way, gather data that provides both useful data insights for the retailer and acceptance by the customer.

But first, why proximity marketing in the first place?

LOCATION / PROXIMITY DATA: *"WHO CARES"?*

With a nudge to the signature *"who cares?"* question the recently deceased Silicon Valley VC pioneer, and founder of Sequoia Capital, Don Valentine asked entrepreneurs pitching to him [1], here are the reasons physical retailers **should** care about gathering this kind of data [2]:

- **Understanding cart abandonment in physical stores** [3]: by using location and proximity data, coupled with data from transactions, brands and retailers can see if a person went to a store and bought something, and then build a profile to re-target them accordingly

- **Location targeting:** Beacons let you target users with messages based on their specific location.

- **Mapping:** The ability to “see” where consumers go in-store and attribute actions to these journeys – e.g. gauge how many buy a product after seeing promotional signs

- **Frequency:** Measure how often people visit the same locations, how long they spend there and how these relate to sales.

- **In-store messaging:** Send promotional offers to people as they look through your store or business location.

- **Guide users:** With full beacon systems, you can guide people through entire shopping centers, stadiums, airports and entire cities.

- **Gamification:** Brands are using beacons to create treasure hunts and gamify the consumer process.

- **Cross-selling / basket size increase:** Target shoppers with related products, special offers and other purchases as they queue up to pay.

- **Loyalty:** Send loyalty rewards to people as they complete purchases.

- **Customer recalls:** Send promotions and other messages to people who leave without buying anything to entice them back into the store.

OPTIONS & CHALLENGES TO GATHER LOCATION / PROXIMITY DATA

We present an overview of the technical options for retailers to gather such data, and some of the recent challenges associated.

RFID

While accurate and energy efficient, there is no RFID sensor in smartphones so the technology is mostly used for physical asset tracking

GEO-IP

A coarse location detection technology with accuracy within a city or metropolitan region based off the IP address a device uses to connect to the internet. It is too coarse for purposes of proximity marketing. Also it requires an active network connection thus making it not so useful to passively detect when a customer comes near a retail venue.

GPS

As the premier location detection technology obviously GPS can be used, but is limited in its ability to track location indoors. It is also relatively high power consumption so the GPS receiver is only turned on when precise location is needed. When an approximate location (accurate within a few 100 yards) or 'significant movement' only needs to be detected (e.g. to determine if someone left the perimeter of a house to activate security cameras or an automatic door lock) triangulation off cell tower signals may be sufficient, not even requiring activation of the GPS receiver in the smartphone. Also note that GPS is one-way, so a smartphone user needs to provide explicit access to a mobile app or website to use this location detection technology, and the smartphone OS requires a similar opt-in even when only cell tower triangulation is used. This is why the use of GPS is generally accepted and not under as much scrutiny as some of the methods we'll discuss next.

BLUETOOTH BEACONS

These are Bluetooth devices that are used as one-way transmitters of some unique identifier that is picked up by a receiving device, such as a smartphone. There is no 2-way communication between beacon and device. There are 2 dominant formats for beacon messaging: Apple's iBeacon format and Google's Eddystone. The Eddystone format is able to send more data than a unique identifier, such as a web URL, while the Apple format can only send unique identifiers and some other system on the smartphone is needed to link that with specific content. Until recently it was possible, as long as you allowed beacon notifications in the Google Chrome browser, to be pinged from nearby beacons, even beacons placed by third parties. You didn't have to opt-in to beacon signals from a specific business or brand. Not surprisingly this led to quite some abuse and it gave beacons 'a bad rep': unscrupulous marketers placed beacons that pushed notifications and web URLs to nearby phones. Google turned off its 'Android Nearby' solution late 2018 [4]. Now you need a mobile app that embeds some code to detect those beacons. Effectively Google adopts the same method for beacon detection Apple has had from day-1: requiring a customer opt-in in the form of installing a mobile app to receive only specific first-party beacon signals.

Recently it's also been found that a lot of apps have been scanning for Bluetooth signals even when the app's functionality doesn't really require it. As part of its improved security and privacy in IOS 13 [5], the version of Apple's iPhone operating system launched in October 2018, a popup notification now alerts a user when an app tries to scan for nearby beacons. Again the age of free-wheeling data gathering without customer benefit is ending.

WIFI DEVICE TRACKING

Also since IOS 13 it is no longer possible for a mobile app to track your location by identifying wireless access points without the customer opting in to location access. Before some apps used the unique identifiers of detected WiFi networks, sometimes in combination with their signal strength, to triangulate a position based on nationwide maps of known WiFi networks. Note that this was done even without the customer actually connecting to any WiFi network.

WIFI ACCESS POINT TRACKING

With specific software embedded in the WiFi access point, it is possible to obtain unique identifiers of devices within the WiFi area. This is because a smartphone, even when not connected to a WiFi network, broadcasts a unique identifier (WiFi MAC address) to check for known networks that it may automatically connect to.

In fact that's how you connect to the WiFi network in a coffee shop in a new city, even when you only went to a similar coffee shop in another city. The WiFi networks in all shops are set up with the same parameters so your phone connects to it since it looks as the same network.

Again Apple here is at the forefront of privacy, although recently Android, in its version P, has caught up: device MAC addresses are being scrambled as long as you're not connecting to a known WiFi network. On Android you need to switch on a 'MAC randomization' option though while on iPhone it is automatically enabled.

However this only applies to unknown WiFi networks. When your phone pings for a known network it connected to before, it actually sends its real MAC address - this is because some WiFi networks, especially in the corporate world, control WiFi access by MAC address.

Several companies use this capability to do audience measurement: detect a number of unique visitors, repeat visitors and their dwell times at a location. To comply with privacy regulations the obtained MAC addresses definitely need to be randomized as they convey certain information about the device (manufacturer, device model) that may be used to identify a user. This is the minimum required to comply with Europe's GDPR rules which prohibit location tracking of individuals via WiFi. Similar regulations can make their way in the US, more about this later.

Because of the link with WiFi access points, it becomes relatively easy to actually identify customers by offering a coupon on a captive WiFi guest login page. As soon as a customer logs in by providing some personally identifying information (typically an email address) to connect to the guest WiFi at one coffee shop, he/she can be tracked at any other location of that chain, or even another retail chain if the guest WiFi is offered by a third party. Would someone expect to be tracked at multiple retail locations without even using their phone there? Surely not. Not surprisingly this is one of the most hotly contested mobile privacy issues currently, and will likely see more protective regulation. There is simply no 'opt-in' for location access via WiFi access point tracking (unlike in the 'device tracking' mode mentioned earlier when the app requests access) since it actually happens unbeknownst to the mobile phone operating system.

Finally the method also has some other limitations even for audience measurement. WiFi network coverage is fairly broad and in retail, unless you're in a big box store, can span multiple stores, on different floors, in a shopping mall. So the accuracy of using the technology to detect the number of visits to your individual retail outlet may be limited.

Time resolution is also limited if a phone is not actually connected to the guest WiFi network: phones only send 'pings' as low as every couple of minutes to save battery power. So the accuracy of using the technology for real-time foot traffic detection is limited.Retailers are advised to understand these issues and potential future ramifications of deploying this kind of technology.

CAMERAS

For simple people counting, several companies use low-cost infrared motion detectors. No privacy issue here but also no actionable data is obtained that can be used to market to those detected 'heat signatures'.

Video cameras can be used for people counting, attribute detection (mood/gender/age range), or full-blow image recognition. Much has been said about the reliability of face recognition and how it may depend on ethnicity, especially when there is no 'enrollment' step. In fact it is much easier to compare if an individual is the same person when he / she voluntarily supplied multiple face scans before to enroll vs trying to detect from different video captures, on different days, under possibly different lighting conditions, hair and grooming styles, if the same person appeared in both shots. Face recognition works for phone login because you first supply multiple scans, from multiple angles, and the best systems use a video camera in combination with an array of special-purpose detectors to detect a 3-D shape of a face.

Therefore in retail today face recognition is largely limited to mood/gender/age range detection, which doesn't uniquely detect an individual and thus is less sensitive from a privacy perspective.

REGULATORY & PERCEPTION ISSUES

As mentioned the *laissez-faire* attitude towards location data gathering by third parties with no relation to the customer is coming to an end. Instigated by the Facebook 'Cambridge Analytica' experience, the discussion is now at the forefront of national political attention. Facebook itself has made significant changes to its API to disallow the data gathering practices that were exposed [6].

We also point out that San Francisco has banned the use of face recognition [7], and that California passed a sweeping privacy bill that goes into full effect in 2020 [8]. The bill guarantees Californians the right to know what data is being collected about them and whether it's being sold or disclosed, and to refuse the sale of their personal information.

So California goes, so likely goes the nation…

So in the end, is at all doom & gloom for proximity marketing? We don't think so. Analytics - only third-party solutions that work unbeknownst to the consumer, and that are only benefiting the retailer or brand, are definitely no longer okay. But we believe the age of first-party proximity marketing has only just begun. With mobile and IOT connectivity, brick and mortal retailers and venues can offer customer-facing solutions that offer a perceived benefit to the consumer/visitor so they can obtain that opt-in, at least when the customer is at (one of their) location(s).

To be successful and socially acceptable in 2020, a proximity marketing solution needs to have a number of attributes, that we'll outline next.

CHARACTERISTICS OF A GOOD PROXIMITY MARKETING SOLUTION

FIRST-PARTY DATA

As a retailer you can control your own (first-party) data collection and its use to limit your liability, now and in the future with more stringent privacy laws.

COMMUNICATE PURPOSE

Clear communication to the customer about what data is being collected and for what purpose.

DIRECT CUSTOMER BENEFIT

Provide a tangible benefit to the customer to obtain the privilege to track presence and make that customer benefit very clear.

An on-premise digital signage network is the ideal vehicle for all of the above: owned & operated by the business, and 'in-the-face' of the customer to communicate both purpose & benefit.

MINIMAL LOCATION DATA

Collect the minimum amount of data: for instance only do presence detection at the business venue, not location tracking outside the venue.

Beacons are ideally suited for this as they only activate the phone when unique pre-registered identifiers transmitted from your own beacons are detected. No indiscriminate scanning of 'all beacons' as was done before, but rather a binary geofence detection for your locations, for which the customer has provided an opt-in. This can be achieved even without installing a mobile app (more about that below). This is a safe and acceptable solution compared to GPS or WiFi network scanning (which picks up all networks).

IN-STORE:

UNIQUE EXPERIENCE

- access to product information or a product offer in retail
- an improved journey in hospitality (eg. reduced wait time via 'skip-the-line' mobile ordering, automated check-in at a restaurant, etc)
- a more personalized experience in the amusement industry (eg. in-seat dining at the movies)

OUT-STORE: FACILITATE DISCOVERY

Use proximity marketing to help customers find businesses of interest to them. For instance, create a local community of local retailers that are not competing with each other but that can benefit from each other's customer base. Vice versa customers perceive the benefit of 'serendipitous retail discovery', stores they didn't know about before but that match their interests.

Proxi.vip

The Proximity Engagement Platform

Proxi.vip is a SaaS service for the retail / hospitality and amusement industries consisting of different parts that can be deployed separately or as a whole. It covers both customer-facing and backend components to marry retail analytics with customer-facing benefits.

Without a customer opt-in, it only supports audience measurement by integrating with a partner's service that provides non-identifying anonymous WiFi audience counting on a WiFi access point.

With a customer opt-in, we can provide customer identification when a customer is nearby by means of presence detection. We do this by placing beacons, with our own unique identifiers, at participating locations. We only track the detection of our beacon signals, not anyone else's. We do not send GPS location or detected WiFi signals (which can cover much larger areas) outside the phone. We don't do continuous location tracking.

Proxi.vip follows a *staircase customer engagement concept:* with low engagement from the customer we can provide a lower benefit, but with higher engagement (typically installation of a mobile app, which could be the retailer's mobile app that integrates our proximity solution) we can do more and provide a bigger benefit to that same customer.

A common misconception is that the detection of beacon signals requires an app on the phone. That is actually not true. Without any app we can still detect that a customer is within the range of one of our beacons to enable the at-location / not-at-location binary detection explained before, and then show a local notification on the customer's phone. But this detection does not leave the phone. Such a local notification is still sufficient to show a personalized message to the user. And this works even when the phone is in lock mode, with the screen switched off: unlike a guest WiFi portal page, the user does not need to open the browser to see a personalized offer or benefit.

Uniquely with proxi.vip, we link mobile interactions, sales receipt data and on-premise digital signage that can be personalized when we have that customer opt-in as we can detect proximity to a signage display, without needing cameras. Without opt-in, we can still contextualize the digital signage based on aggregate historical sales or visit patterns.

We invite you to find out more about us and the components of our Proxi.vip platform by visiting our website at www.sophatar.com or www.proxi.vip. Come see us at our booth#708 on Level 3 during NRF's The Big Show at the Javits Center in New York, January 12-14 2020.

References

[1] "Remembering Don Valentine", Sequoia Capital, Oct 25 2019, https://www.sequoiacap.com/article/remembering-don-valentine/

[2] "Google Beacons: Proximity marketing is ready to take off in 2019", Vertical Leap, Nov 14 2018, https://www.vertical-leap.uk/blog/google-beacon-proximity-marketing/

[3] "The real-world abandoned shopping cart", Retail TouchPoints, Feb 14 2018,

https://www.retailtouchpoints.com/features/executive-viewpoints/the-real-world-abandoned-shopping-cart

[4] "Discontinuing support for Android Nearby notifications", Android Developers Blog, Oct 25 2018,

https://android-developers.googleblog.com/2018/10/discontinuing-support-for-android.html

[5] "IOS13: top 5 new security and privacy features for your iPhone", cnet.com, Sep 22 2019, https://www.cnet.com/how-to/ios-13s-new-privacy-features-help-keep-your-location-a-secret/

[6] "A guide to the new privacy changes at Facebook", Silicon Republic, Apr 5 2018, https://www.siliconrepublic.com/enterprise/facebook-data-privacy-settings

[7] "San Francisco bans facial recognition", NY Times, May 14 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[8], "California Consumer Privacy Act (CCPA)", State of California Dept of Justice, https://oag.ca.gov/privacy/ccpa

SOPHATAR

2 North First St, 5th floor
San Jose, CA 95113
844-469-7674
info@sophatar.com
www.sophatar.com
www.proxi.vip