



# DIGITAL SIGNAGE GROUP

Best Practices:  
Recommended Code of Conduct for Consumer Tracking Research



## **TABLE OF CONTENTS**

1. Introduction
2. Methods of OTD Collection
  - 2.1 Low Risk OTD Collection Methods
  - 2.2 Medium Risk OTD Collection Methods
  - 2.3 High Risk OTD Collection Methods
3. The Code of Conduct
  - 3.1. Data Collection, Storage and Security
  - 3.2. Disclosure
  - 3.3. Cross-Channel and Cross-Domain Marketing
4. Participation

### **SUMMARY**

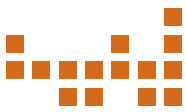
While technology imposes few restrictions on data collection in retail settings, marketers should safeguard consumer privacy. This document provides recommendations to marketers on maintaining ethical boundaries with consumer data and suggestions on how consumer observations and marketing insights should be collected and used.



## **1. INTRODUCTION**

Technological advances have made it effortless and inexpensive to track consumers in stores using surveillance or other types of camera or recording media. On the one hand, there is huge demand to gather shopper insights in order to profitably market the right products to the investing consumer and provide a hassle-free shopping experience. On the other hand, the ability to record and track the consumer's every move through the store, identify consumers facially and demographically, and pinpoint where and what customers are looking at, picking up, and putting into their shopping carts through Observed Tracking Data (OTD) raises privacy issues and sends shivers down the spine of even the boldest marketer. While the federal government has recognized the dangers of gathering and using personally identifiable consumer information in the realm of mobile marketing and healthcare and has subsequently passed laws to protect consumers, there are no such laws that currently exist for data collection in retail settings.

Therefore, there is a clear need for guidelines on data gathering and storing so that consumers are protected and the ethical boundary is maintained. For instance, it may be good business practice for marketers to track purchases through loyalty cards, or track how many people paused before a certain display. However, it may not be okay to record and store facial data for marketing purposes without the consent of the consumer. Consequently, this document was created to provide recommendations on collecting data in ethical manners and to encourage marketers to consider ethical issues before they even begin to collect data. This document is not meant to be a replacement for federal and state laws; federal and state laws obviously take precedence over this document and should always be consulted and followed to ensure compliance with the law.



## **2. METHODS OF OTD COLLECTION**

Before considering recommendations, it is important to understand and categorize different OTD collection mechanisms by the degree of privacy exposure they may create for the consumer. Once the level of risk is ascertained and understood, measures can then be taken to protect consumer privacy. In a nutshell, there are three major levels of risk: low, medium, and high. Typically, low risk methods do not track individual consumers nor do such methods gather identifiable data. Medium risk methods gather individual tracking data but do not identify consumers. High risk methods identify customers in the process of tracking them.

### **2.1 LOW RISK OTD COLLECTION METHODS**

- Infrared or laser beam motion detectors
- Sonar and other non-recording, sound-based motion detectors
- Overhead path tracking systems that are capable of generating on-premise, aggregate “heat maps” of consumer presence, but are not able to track or record individual consumer paths.

### **2.2 MEDIUM RISK OTD COLLECTION METHODS**

- Overhead camera-based path tracking systems or “gaze tracking” systems that are able to track and/or record individual consumer paths, but do not uniquely or individually identify consumers.
- Sensor-laden shopping carts that track and/or record individual consumer paths, but are not able to uniquely or individually identify consumers.
- RFID or other wired or wireless tracking devices knowingly worn or carried by consumer, or used on shopping carts and baskets to track consumer behavior, but are not able to personally or uniquely identify consumers.
- Any method where information can be used to collect demographic or psychographic information, but cannot be used to individually or uniquely identify consumers.



---

## **2.3 HIGH RISK OTD COLLECTION METHODS**

- Personally identifiable OTD collection via mobile phone or mobile computing device via wireless (cellular, Bluetooth, etc.) connection.
- Any method capable of identifying consumers based on past purchases, loyalty card programs, or other behavioral patterns collected by OTD collection methods.
- Any camera-based OTD system that collects and stores visual data.
- Any method used to personally or uniquely identify consumers, when combined with loyalty program data, or 3rd party marketing data.



## 3. THE CODE OF CONDUCT

This Code of Conduct describes three categories of recommended practices for OTD collection and marketing activities:

- 3.1) Data Collection, Storage and Security,
- 3.2) Disclosure, and
- 3.3) Cross-Channel and Cross-Domain Marketing.

### 3.1. DATA COLLECTION, STORAGE AND SECURITY

- OTD collection venues that house HIPAA-compliant entities (for example, a supermarket that contains a pharmacy) must adhere to all Federal laws governing the collection and use of marketing data in and around HIPAA-compliant sites. Typically, OTD collection methods may not be used in the HIPAA-compliant areas themselves, and special care must be taken to ensure that no method that allows for the unique or individual identification of consumers is used to track consumer behavior near the HIPAA sites. [Click here](http://www.hipaa.org) or visit [www.hipaa.org](http://www.hipaa.org) to learn more.
- OTD collection mechanisms capable of uniquely identifying a minor (i.e., a consumer under 13 years of age or the age required by state or local law) cannot be used at the OTD collection site.
- In no event should image, video or biometric data used to generate OTD be stored without an explicit consumer opt-in to do so. Collecting image or biometric data for marketing purposes may violate Federal, state or local laws, including Federal Domestic Violence Laws. If collecting image or biometric data is allowed in a venue's jurisdiction through OTD methods, the data should be stored for up to 3 months or the maximum period allowed by law.
- Using video or image data from surveillance, security, or loss-prevention systems may violate Federal, State and/or local laws, and is generally not recommended. If this practice is allowed by law, marketers must use separate computer




systems and storage devices from those used to store the security/surveillance data. These computer systems and storage devices must be password protected with different passwords used than for the security/surveillance systems. Great care should be taken to protect this data against theft or unlawful access.

- Any and all collected OTD that can be positively associated with a unique consumer should be treated as Non-Public Personal Information (NPPI), and must be stored on a sufficiently secure computer system, such as one that conforms to the Payment Card Industry (PCI) standards for NPPI storage. Any OTD that could potentially be misused to create public safety hazards must be treated as NPPI and be handled as described above. Again, great care should be taken to ensure privacy of this data.
- It is a violation of Federal law to use certain types of marketing data (for example, demographic data) to offer special promotions to one group of consumers but not another. Marketing practices that make use of demographic or psychographic OTD may not be used to create promotions that vary the pricing, availability, or access of an item or items, or change requirements and availability of financing options, if applicable.
- Please [click here](#) or visit <http://www.consumerprivacyguide.org/law/> for brief information on consumer privacy laws. Please visit the Federal Trade Commission's website at <http://www.ftc.gov/bcp/about.shtm> to learn more about laws surrounding consumer rights.

### **3.2. DISCLOSURE**

- Marketers must provide a disclosure notice to consumers who may be monitored (intentionally or incidentally) by OTD activities.
- The disclosure notice should be easy to understand,



---

---

unambiguous, and current. It should not contain any false or misleading information about the nature of the OTD collection methods or the intended use of any collected data.

- The disclosure notice should describe the OTD collection methods in effect and whether data collected via OTD methods will be combined with other data including, but not limited to, register receipt information, credit card information, any NPPI information or data collected by 3rd party and/or affiliate marketers.
- The disclosure notice should be posted in at least one location at each site where the OTD collection is taking place, preferably at every entrance.
- The disclosure notice itself must meet all ADA guidelines and must be free of obstructions that might inhibit visibility.
- The disclosure notice must contain information about all available opt-in and opt-out mechanisms such as a consumer-accessible telephone that can be accessed for no fee in order to opt out.
- When OTD requires the use of a consumer's cell phone, mobile computing device, email messages, SMS text messages, or links OTD data with a telephone number or Bluetooth device, marketers must also comply with the Mobile Marketing Association's Global Code of Conduct, mobile marketing laws, FTC Telemarketing Sales Rule, other FTC rules, and the National Do Not Call Registry.

### **3.3. CROSS-CHANNEL AND CROSS-DOMAIN MARKETING**

- Cross-channel OTD marketing occurs when data from multiple sources, such as in-store, catalogs, online, and OTD are combined with the intent of tracking a consumer across multiple properties, retail environment, or other public or private spaces.
- Consumers should be made aware of the use of their OTD



data and other marketing data. Such information should be included in the Notice.

- Cross-channel marketing is considered High Risk for OTD collection mechanisms. Therefore, consumers should opt-in before data is combined in cross-domain ways. Furthermore, the consumer should also re- opt-in to the program each time he or she enters a new venue where the cross-domain OTD marketing program is ongoing.
- Disclosure notices should be located at every OTD collection site participating in the program, and should follow all other best practices for OTD data collection.
- Disclosure notices for cross-domain OTD marketing programs must contain a complete list of all marketers and other entities participating in the program (for OTD collection or other purposes), as well as a complete list of all OTD collection practices and the physical locations of the OTD collection devices.



## **4. PARTICIPATION**

This document is not a contract or legal document, and therefore is non-binding. However, adherence to the Code is strongly recommended to ensure that consumer privacy is safeguarded. Marketers should be conscientious in the manner by which they gather and use consumer data, and should take precautions to safeguard consumer rights.

