

Collecting Data “IRL”: A Practical Approach to Mitigating Risk when Collecting Offline Data for Online Use

Susan Israel, Of Counsel

Jessica B. Lee, Partner, Co-Chair, Privacy Security &
Data Innovations

sisrael@loeb.com

jblee@loeb.com



We Should All Have a Good Idea About What's Required When Collecting Data Online...



cookies

This page uses cookies: [Read more](#)

Alright

LANCÔME
PARIS

1. My shopping bag ——— 2. My order

Identification

Enter your e-mail

If you already have an account, [click here to modify your e-mail](#).

Your first name*

Your surname*

Please confirm your e-mail*

☒ I would like to subscribe to the Lancôme newsletter to receive the latest news. Lancôme does not share or sell your personal information

CONFIRM



But What Happens Offline or “IRL”?



Stadiums Retail, Bulletin Boards and Other Spaces Are Ripe for Data Collection

Beacons

Point of Purchase

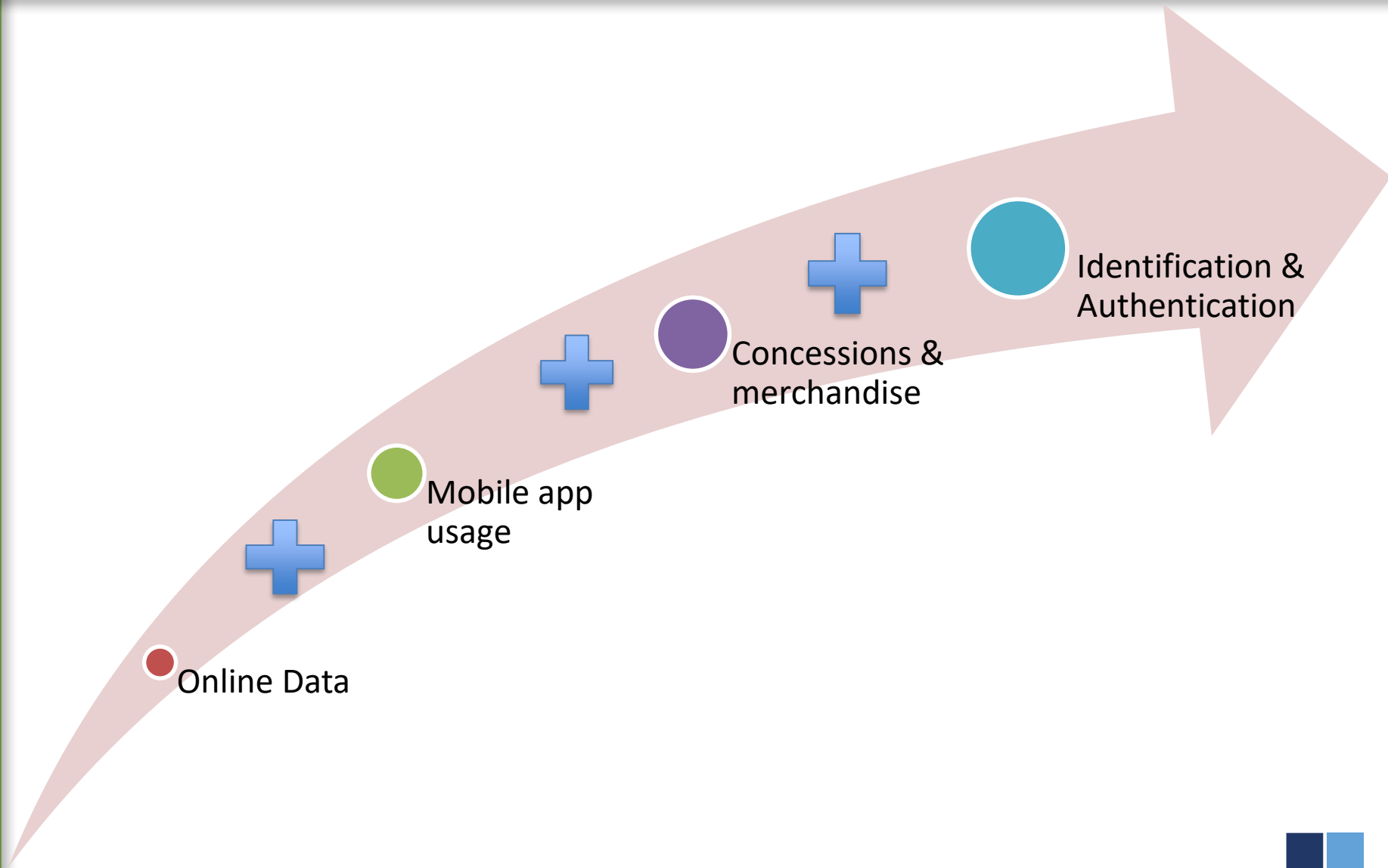
RFID

Sensors

Mobile Apps

CCTV

This Offline Data Can Be Used to Enrich Data Collected Online



Case in Point: Walgreens Intelligent Retail Lab (“IRL”)

- Employs thousands of high resolution cameras, which can be combined with sensors on shelves, to monitor the store in real time so its workers can quickly react to replenish products or fix other problems
- Disclosures are provided throughout the store
 - Signs note that the store is testing cameras and sensors that "do not identify you or store any images" and includes links to a privacy policy



Consider the Consumer's Expectations

Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, which may include:

- ✓ product and service fulfillment;
- ✓ internal operations;
- ✓ fraud prevention;
- ✓ legal compliance and public purpose; and
- ✓ first-party marketing.

Examples: Scanning a ticket on entry, taking a credit card for payment for merchandise

Practices a Consumer May Not Expect

- Using purchase data for advertising
- Collecting location data when a consumer believes she has turned off location
- Publication of name or likeness (example interactive billboard on sidewalk)
- Re-use of a souvenir photo
- Retention/Re-use of ID/Authentication Data for Secondary Purposes

What's Required?

- Online or Offline, the Fair Information Practice Principles Still Apply
 - ✓ **Transparency & Purpose Specification.** Consumers should be given notice that their data is being collected, how it is collected and how it will be used.
 - ✓ **Choice.** Consumers should be given the option to control whether their data will be used to build their consumer profile, or other marketing and advertising purposes
 - ✓ Data Minimization, Data Quality and Integrity, Security, and Accountability should also be considered.

Consider Relevant State Laws & Self-Regulatory Frameworks

- NAI's Updated 2020 Code
 - Now includes rules specific to the collection of offline data
- State Biometric & Facial Recognition Laws
- Laws Regulating CCTV and Recording in Public Spaces
- Rights of Publicity
- FTC's 2012 Privacy Report

Special Considerations for Sensitive Data

- Special or other “sensitive” categories of data, including biometric data and precise location information will require opt-in consent.
 - ✓ If you use biometrics for authentication or identification, you may need to provide an alternative options for consumers who do not opt-in.
 - ✓ Parental consent will be required to collect this information from children.
- Consider: the NAI considers information identifying the space in which a person is located to be “precise,” despite its size. (e.g. “Madison Square Garden”)

Best Practices: Providing Transparency and Giving Choice

“IRL”

The challenge with IRL data collection is often the lack of a screen or other space to provide notice. Map out the consumer journey and identify when data is collected and the options for providing notice based on the space.

- Online ticketing
 - If you first encounter your user online, consider disclosing the offline practices at your ticketing screen or other window, prior to the consumer entering the premises.
- Onsite Fingerprints/Retina Scans
 - Identify a place on the scanner where information can be provided and train attendants to answer visitor questions and provide information about how data is used
- Mobile Apps
 - If your app is designed to enhance a consumer's experience in your venue, include disclosures in the app store and the mobile app privacy policy

Best Practices: Providing Transparency and Giving Choice

“IRL”

- RFID and other wearables
 - Use the screen or the packaging to disclose any relevant privacy information and provide a link to the company’s privacy policy
- CCTV/Cameras
 - Use “crowd release” signs to inform consumers that cameras are being used and provide them with a website they can use to get more information or exercise any choice options
- Consider A Frames and other physical signs

Remember: Don’t surprise the consumer by referencing offline behavior in online ads

Best Practices: Security, Data Minimization, Data Integrity

- Offline data requires the same data subject access rights, and the same security as online data
- Limit data retention
- De-identify, hash or truncate identifiers where possible
- Remember affiliates are third parties unless their relationship is obvious to the consumer

Key Takeaways

- ✓ Limit data collection – consider what you “need”
- ✓ Follow the same fair information practices you use online for offline data collection
- ✓ Obtain consent prior to reusing data in a different channel or with a different affiliate unexpectedly unless you have a method (online, can be before event, on ticket sale agreements) to obtain consent
- ✓ Obtain consent to use images for publicity
- ✓ Use signs where necessary
- ✓ Rely on opt-in audience samples where possible
- ✓ Know your local laws, know your vendors
- ✓ Offer alternatives to biometric identification, if biometric information is to be collected (with consent)

Questions ???