



# Advertising and Promotional Communications in a Mobile World

## Cross-Device Tracking

**Kristi Wolff**  
Partner, Kelley Drye & Warren

# Single Device vs. Cross-Device Tracking

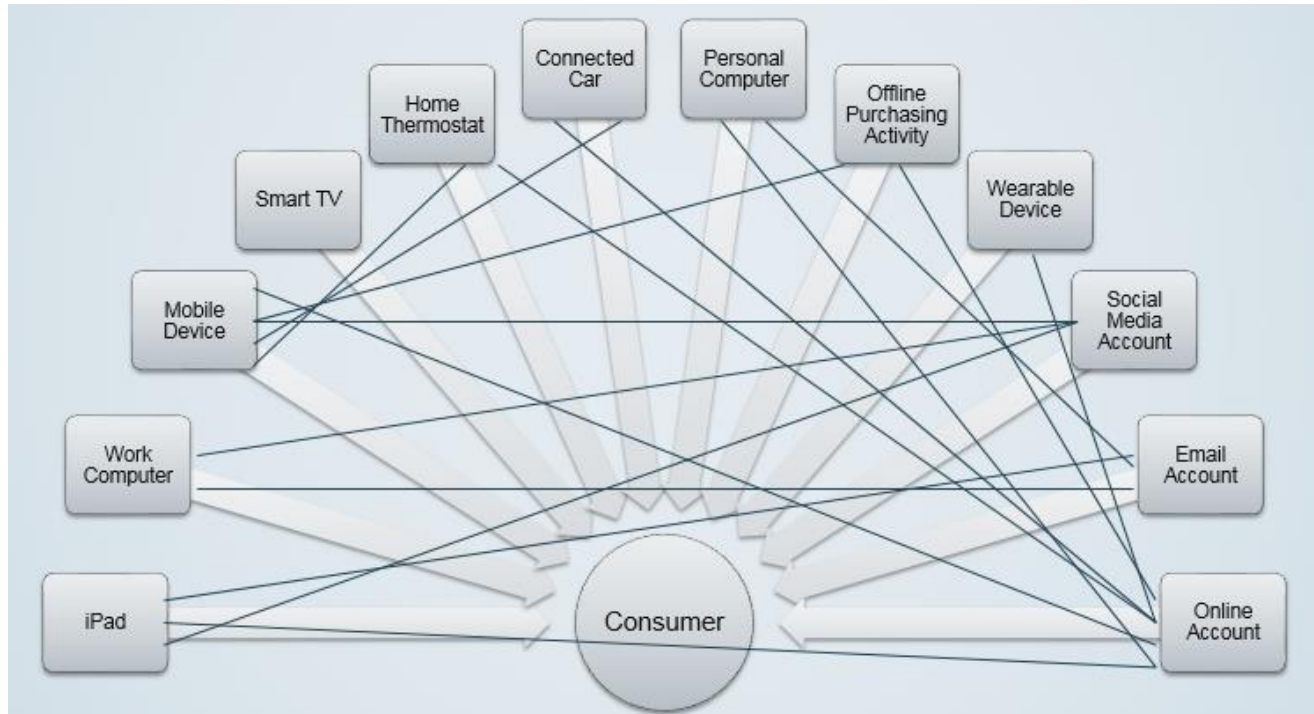
- **Single Device OBA**
  - Browsing for shoes on a desktop computer, and then later targeted for an ad on same computer for shoes
- **Cross-Device Tracking**
  - Browsing for shoes on a desktop computer, and then later targeted for an ad on a tablet which has been “linked” to the same user



# What is Cross-Device Tracking?

- Tracking a consumer's online activity among various devices, apps, and browsers to create a more-detailed user profile than what is available through cookies alone
- **Deterministic Linking (DL)**
  - Persistent identifier -- user logs in to app, platform, etc. on devices
  - Accurate but limited reach
- **Probabilistic Linking (PL)**
  - Build a graph based on statistical/predictive models
  - IP address, WiFi networks, location, websites browsed, ads displayed, device type, operating system, cookies, mobile device IDs, time of day, etc.

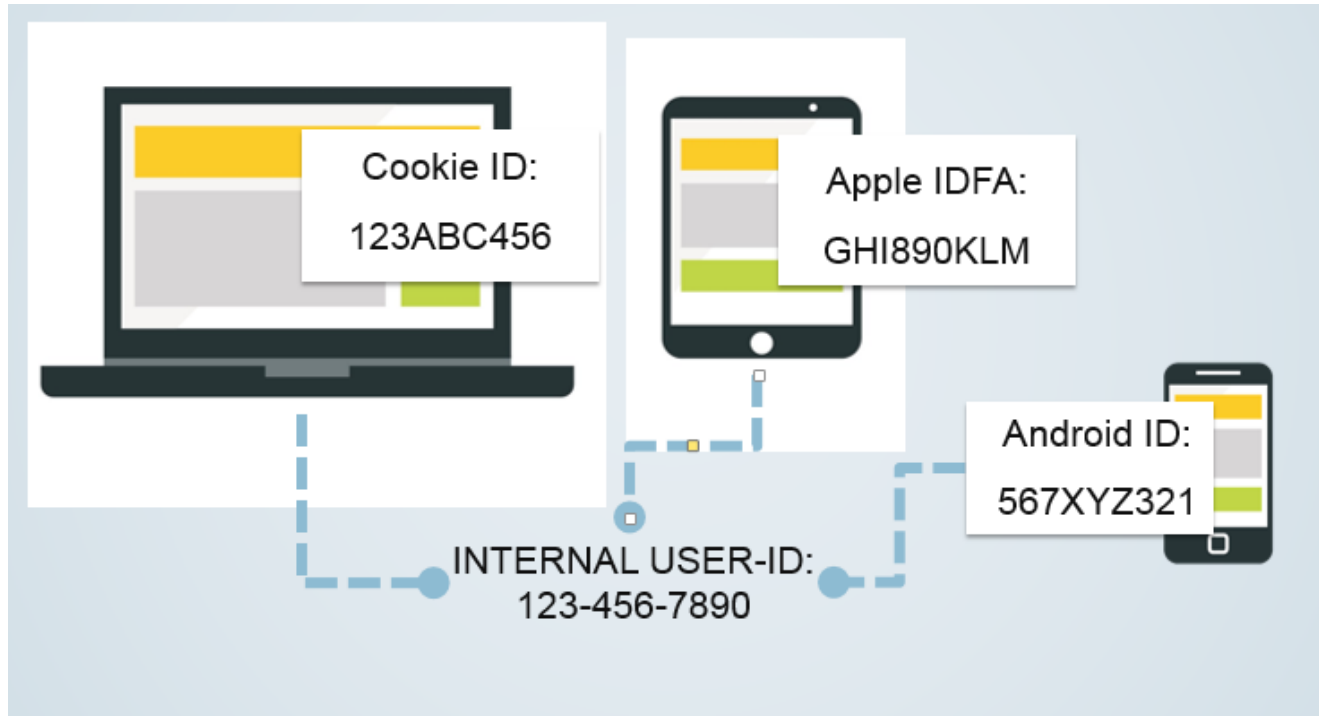
# Potential Cross-Device Profile Sources



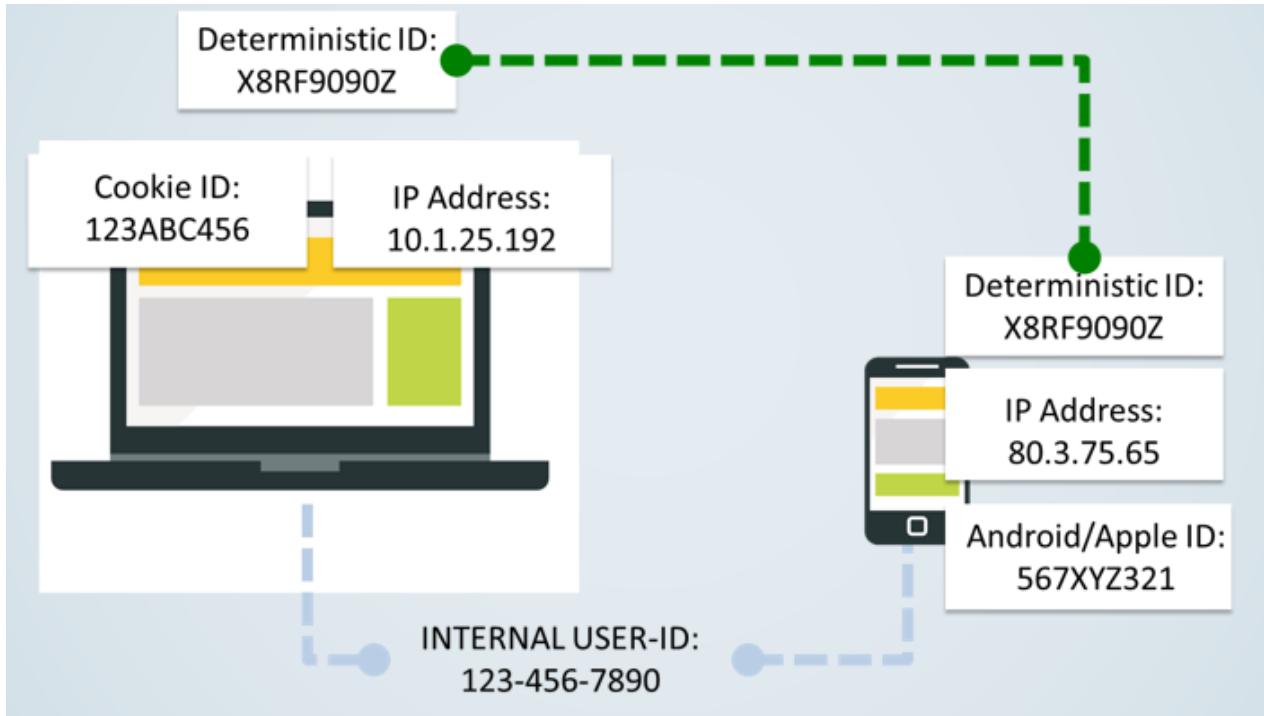
# Benefits of Cross-Device Tracking

- **Marketing benefits**
  - More ways to reach a consumer
  - Better targeted ads/offers (content, format, location, timing, frequency)
  - Cap the number of times a consumer sees the same ad
  - Better attribution
- **Interoperability benefits**
  - Users can seamlessly pick up where left off on one device, or have the same bookmarks in the browser
- **Fraud prevention**
  - Learn which devices typically access consumer accounts, or send alerts when new devices are used to access accounts

# How Cross-Device Tracking Works



# How Cross-Device Tracking Works



# How Cross-Device Tracking Works



- Click on an article about the best beaches in Tahiti

On Work  
Desktop

On Phone

- On the train home, you use your browser to search for “cheap hotels in Tahiti”

- Logged in to a social media site at home, served an ad for a “flash sale” for flights to Tahiti, and buy the tickets at a great price

On iPad





# How Cross-Device Tracking Works



- Click on an article about bipolar disorder

On iPad

On Phone

- Use the browser to search for "psychiatrists in DC"

- An ad for a drug intended to treat the mental illness appears, boss sees it

On Shared Work Laptop

# FTC Staff Report (Released Jan. 23 2017)

## AN FTC STAFF REPORT

Federal Trade Commission  
January 2017



- Describes the FTC's November 2015 Cross-Device Tracking Workshop
  - ✓ How cross-device tracking works
  - ✓ The benefits and challenges of cross-device tracking
  - ✓ Industry efforts to address the privacy and security implications of this practice
- Recommendations to businesses on how to apply the FTC's longstanding privacy principles to cross-device tracking

# DAA Self-Regulatory Framework

- About DAA and NAI
- Two key principles: transparency and consumer control
- November 2015 guidance: Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices
  - Enforcement began February 1, 2017
- NAI considering best practice recommendations
  - Application of Choice
  - Transparency



# Best Practices for Cross-Device Tracking

- Transparency/Disclosure
  - Provide truthful disclosures to consumers and to the first-party companies on whose websites and apps they appear, so that these first parties can in turn make truthful disclosures to consumers
  - Disclose data collected, data transferred to third parties, collection of precise location data
- Control/Choice
  - Opt-out to cover all linked browsers/devices as a best practice vs. per-device
  - Some have advocated for a single opt-out that would apply across consumers' browsers, smartphones, tablets, and smart devices, but technical challenges and other concerns

# Best Practices for Cross-Device Tracking

- Sensitive Data
  - FTC staff recommends that companies refrain from engaging in cross-device tracking on sensitive topics, including health, financial, and children’s information, without consumers’ affirmative express consent
  - NAI Code requires members to obtain consumers’ opt-in consent before using sensitive data or precise location information for interest-based advertising
    - NAI Code defines sensitive health information broadly as “information, including inferences, about sensitive health or medical conditions, or treatments.”
- Security
  - FTC Act requires companies to maintain reasonable security
  - Keep only the data necessary for business purposes
  - Properly secure collected and maintained data