

ALSTON
& BIRD



Volume, Velocity, Variety: Vendor Management in an IOT/VR/AI Digital Age

June 13, 2017

Dominique Shelton



AGENDA

- How Do We Use Vendors?
 - Mobile Apps/Video
 - Emerging trends
 - IoT
 - Artificial Intelligence
 - Augmented Reality
 - Virtual Reality
- Threats Posed by Vendors
 - Regulatory
 - Litigation
- Controlling/Limiting Risks Through Vendor Management
 - In-Take



IoT and Video





IoT: The New AI App Stores

GeekWire

NEWS ▾

JOBS

EVENTS ▾

RESOURCES ▾

DEALS

ABOUT ▾



Search



Trending: Medical startup once backed by Jeff Bezos and other high-profile investors reportedly closing

Amazon's smart assistant Alexa now tops 7,000 skills, a 7X increase in 7 months

BY NAT LEVY on January 4, 2017 at 10:31 am

Post a Comment

f Share

Tweet

Share 587

Reddit

Email

Sponsored by

Northeastern
University
Seattle

The GeekWire team is covering CES 2017 live from Las Vegas, featuring the latest in consumer electronics, cars, sports tech and more.

GeekWire Cloud Tech Summit tix here!

Ad closed by Google

Stop seeing this ad

Why this ad? ▶





IoT: Artificial Intelligence

THE WALL STREET JOURNAL

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

Search

Netflix's Global Growth Fuels Surge in Subscribers

Court Denies Arrest Warrant for Samsung Heir Lee Jae-yong

U.S. Sues Oracle, Alleging Salary and Hiring Discrimination

FCC's TV Airwaves Auction Nears End With About \$18 ...

PERSONAL Call Democ Against?

TECH

Talking Dolls May Spread Children's Secrets, Privacy Groups Allege

Complaint alleges My Friend Cayla and I-Que Intelligent Robot collect and use personal information from children



Advocacy groups allege that Internet-connected toys, including several children's dolls, pose a privacy risk to consumers. WSJ's Georgia Wells explains on Lunch Break with Tanya Rivers. Photo: Getty

By **GEORGIA WELLS**

Updated Dec. 6, 2016 7:26 p.m. ET

6 COMMENTS

POWER YOUR CLIENTS PORTFOLIO WITH QQQ





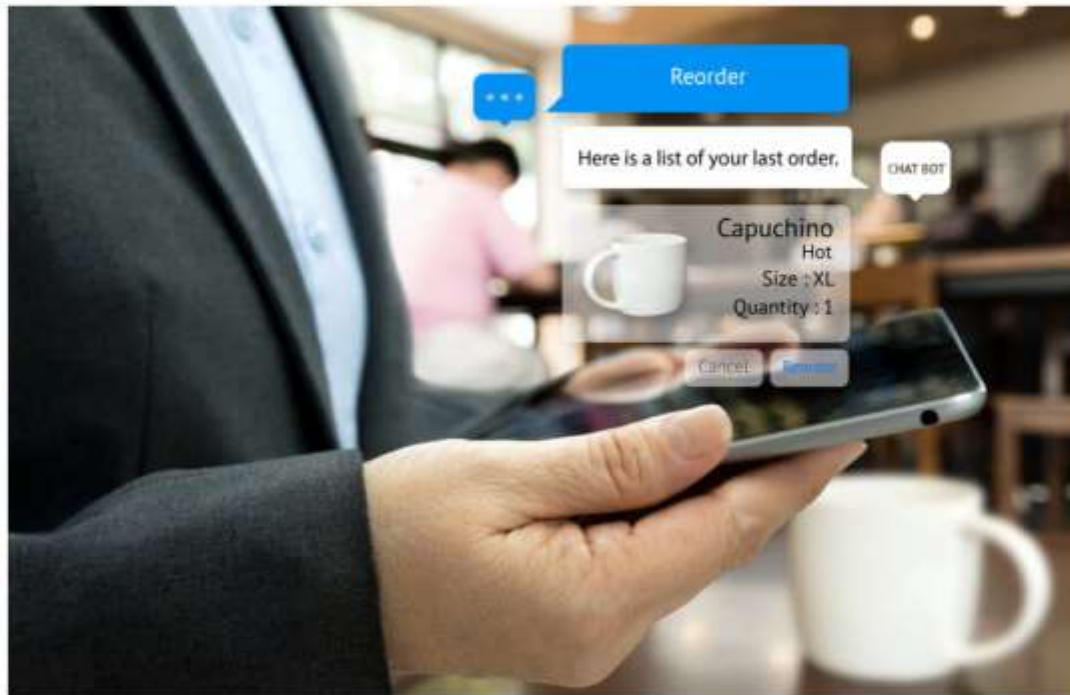
IoT: Artificial Intelligence

BOTS

GUEST

4 big problems plaguing chatbots

NIKHIL VIMAL, STREETBASH @NIKIVIMAL JANUARY 18, 2017 4:10 PM



Right now is a prime time to launch a **chatbot**. There are a handful of good bots,

Above: Fix these chatbot problems.



Wearable Tech (Projected \$24 billion industry by 2020)



'Electronic skin' to monitor your health

Researchers in Japan have developed "electronic skin" with an organic circuit that can be worn on the human body. It is 10 times thinner than a skin cell and lighter than a feather.

It has many potential uses including monitoring your health, it could be worn as an electronic tattoo or in the future generate a television picture on your hand.

Prof Takao Someya of Tokyo University explained to **BBC Click's** Dan Simmons how it works.

04 Apr | Technology

Share





Augmented/Virtual Reality Movies Reported April 16, 2017

« [What's the Game Plan for the Ever Aggressive Foxconn?](#) | [Main](#) | [South Korean Firms are big Winners for the iPhone 8](#) »

April 16, 2017

A Major Warner Bros. Patent Reveals a Coming AR/VR Movie Delivery System for Theaters, Home systems & Headsets

Patently Apple



patentlyapple.com/patently-apple/

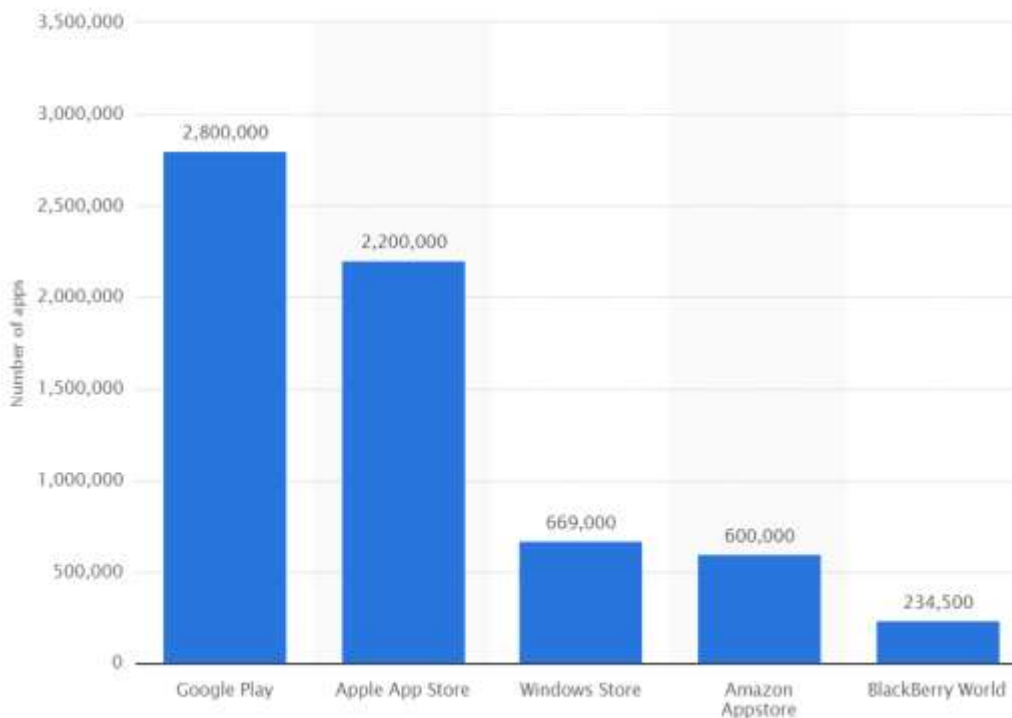


Over 5 million Mobile Apps Available in Apps Stores-2017

Industries › Internet › Mobile Internet & Apps › Number of apps available in leading app stores 2017

Number of apps available in leading app stores as of March 2017

PREMIUM +



ABOUT THIS STATISTIC

This statistic contains data on the number of apps available for download in leading app stores as of March 2017. As of that month, Android users were able to choose between 2.8 million apps. [Apple's App Store](#) remained the second-largest app store with 2.2 million available apps.

[Show more...](#)

SPECIAL FUNCTIONS

Download as ...

- Graphic (PNG) +
- Excel (XLS) +
- PowerPoint (PPT) +
- PDF +

Options

- Settings +
- Print +
- Research Alerts +



Television Apps

tom's guide

PHONES LAPTOPS CAMERAS TV GAMING WEARABLES FORUM ALL PRODUCTS +

APPS > ROUND-UP

17 Best TV Apps

by JOHN CORPUZ Apr 13, 2016, 8:22 AM



Ad closed by Google

Stop seeing this ad Why this ad? ▶



17 Best TV Apps

Smartphones and tablets can add to the big screen TV experience, with "second screen" apps allowing users to search for supplementary information such as series synopsis, cast details and schedules. In addition to TV companion apps, selected channels and networks are even releasing apps that allow you to stream content right after release. And of course, subscription streaming services such as Netflix and Hulu are putting viewers on cloud television.



What is Cross-Device Tracking





Deterministic Cross-Device Tracking

- Customer Relations Marketing
 - Login
 - Emails
- Plus behavior
- Plus Device



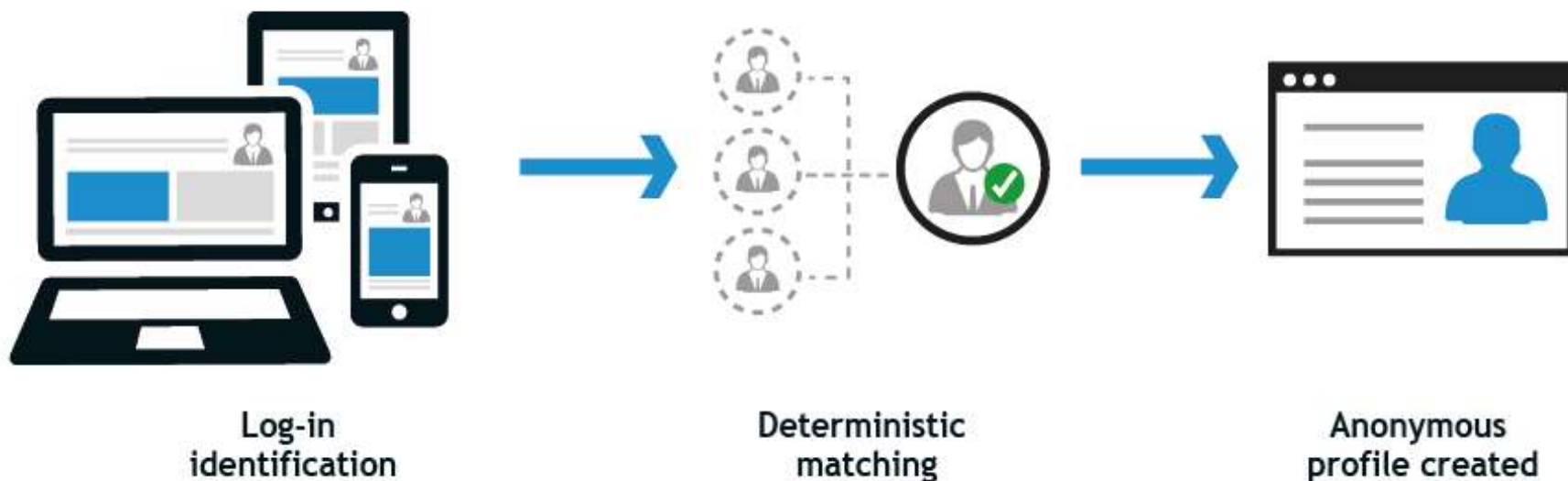
5 Tips For Executing Cross-Device Targeting

Experts share how to get the most from data-heavy campaigns By Marty Swant



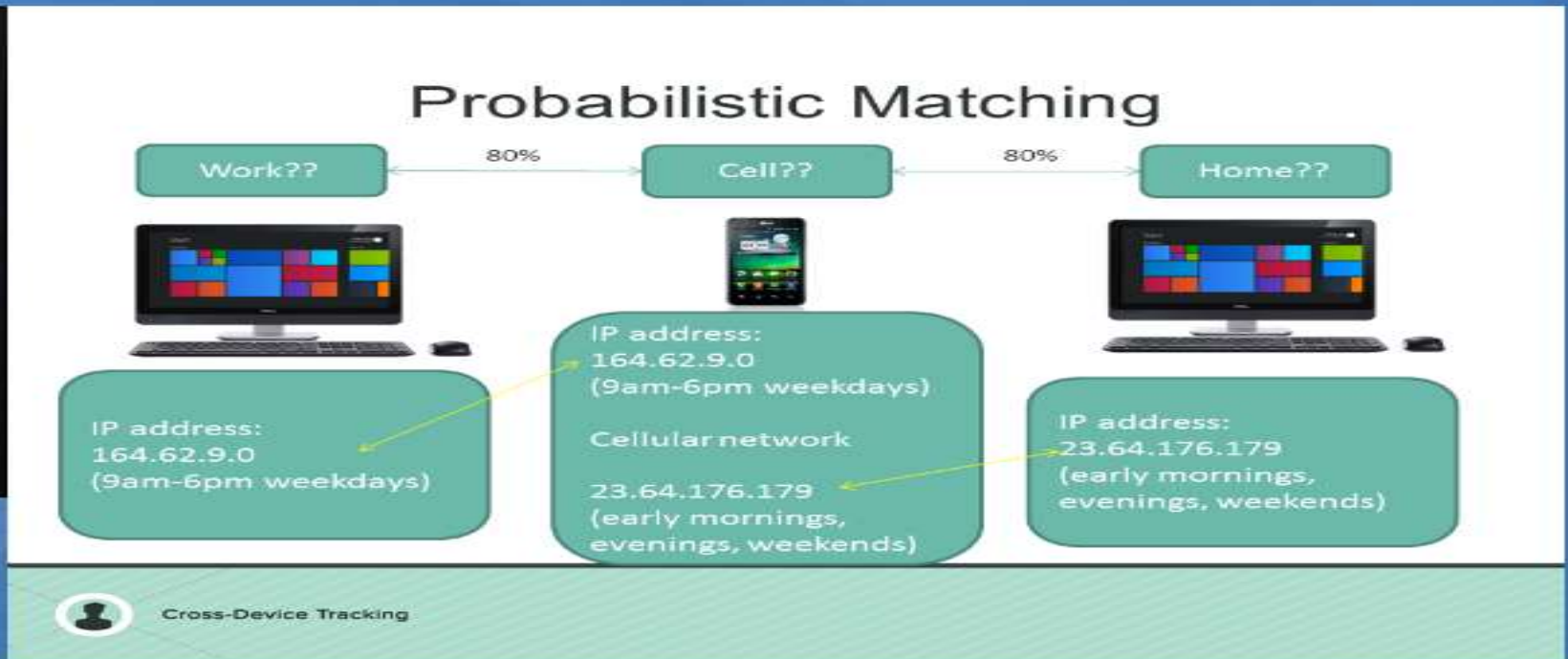


Deterministic – User is Known





Probabilistic Fingerprinting



- Probabilistic tracking often includes device attributes like operating system, device make and model, IP addresses, ad requests and location data, and making statistical inferences to link multiple devices to a single user. Proprietary algorithms are often used



FTC Cross-Device Tracking Jan. 2017 Report



AN FTC STAFF REPORT

Federal Trade Commission
January 2017





Privacy & Data Security Threats Posed by Vendors

June 13, 2017

Dominique Shelton



Pokémon Go – Lawsuit defeated on May 3, 2017- lack of injury

- July 27, 2016, plaintiff filed a putative class action lawsuit in Florida after a researcher discovered that the app asked iPhone users for permission to access their Gmail accounts, contacts, and other information stored in Google's cloud. (Niantic said that request was the result of a glitch, and that the app only accessed people's User IDs and email addresses.)

MediaPost

News

Events

Awards

Members

More



Pokemon Go Defeats Lawsuit Over Privacy Policy

by Wendy Davis @wendydavis, May 3, 2017



Siding with the developer of Pokemon Go, a judge has dismissed a consumer's lawsuit over the app's privacy policy.



FTC Complaints

- By September 2016, 72 consumer complaints filed with the FTC. *See, Spurned Pokemon Go players file complaints with federal government, available at <https://www.polygon.com/2016/9/28/13082056/pokemon-go-ftc-complaints>*
 - “The Pokemon Go mobile game privacy policy states that they access ‘PII such as email address’ but their app requires FULL google account access to function - giving them access to all emails, calendar contents, contacts, etc. At no time when creating an account or linking the game to one’s google account does the app state the extent of the access or that the required access far exceeds that described in the privacy policy. Revoking access from one’s google account forces the game to log out and logging back into the game reinstates full google account access. This game is aimed at children and very aggressively deceives players into revealing potentially incredibly private information.”



This is Not the Only Case...

- Developers sued for trespass

- New Jersey

- Calgary

- California

Lawsuit targets Pokemon concerns 5

Calgary lawyer files class action on behalf of frustrated homeowners

Calgary Herald 11 Aug 2016 +9 more

KEVIN MARTIN

Barbie Schaeffer wishes the developer of Pokemon Go would just leave her alone.

The Torrington woman said Wednesday her home in the sleepy hamlet northeast of Calgary has been inundated with un-

wanted visitors ever since her property was designated a Pokemon Gymnasium last month.

"If this (address) was taken off the game it would be back to sleepy hollow," she said of the quiet hamlet east of Olds on Highway 27.

Schaeffer said she went to the Pokemon Go website and sent a letter of complaint, but received only a form letter back saying her complaint would be looked into.

"We're in a small town," she

said. "We don't want this l attention.

"On the weekend we h other wave of people through," Schaeffer said.

"Someone flew a dron the backyard on Saturday."

She said game players even tried scaling her fence a better chance at catch Pokemon figure — whic driven her two dogs to d tion.

"The dogs are los



Emerging Technologies – Causing New Privacy Litigation Risks

- **Tracking for Ad Tech and Analytics:** Over 200 privacy class actions filed. Mobile apps are increasingly the focus. 265 mobile app privacy cases filed since January 2016 in the US.
 - Europe creates new risks May 25, 2018.
- **Internet of Things:**
 - **Smart TVs** – *In re Vizio Inc. Consumer Privacy Litigation* (8:16ml2693, Central Dist. California) (16 cases MDL)
 - **Connected Car** - *Cahen et al. v. Toyota Motor Corporation et al.* 2015 U.S. Dist. Lexis 159695 (C.D. Nov. 25, 2015).
- **Text Messaging**, A reported 4,860 class actions filed in 2016. *Year in Review: Consumer Litigation Filings End 2016 with Surge in TCPA Cases* (<http://www.acainternational.org/news/year-in-review-consumer-litigation-filings-end-2016-with-surge-in-tcpa-cases>)





***In re Nickelodeon* 2016 U.S. App. Lexis 11700 (3rd. Cir. Jun 27, 2016)**



Regarding Nickelodeon's mobile app: Third Circuit finds harm after Spokeo – but MTD granted because no specific disclosures of Video Viewing.

“The purported injury here is clearly particularized, as each plaintiff complains about the disclosure of information relating to his or her online behavior. While perhaps "intangible," the harm is also concrete in the sense that it involves a clear de facto injury, i.e., the unlawful disclosure of legally protected information. Insofar as Spokeo directs us to consider whether an alleged injury-in-fact "has traditionally been regarded as providing a basis for a lawsuit,"⁶³ Link to the text of the note Google noted that Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private.” ^{*63-*}64.



Some FTC Enforcement Actions





Know Regulatory Enforcement Actions – And the Topics Covered Relevant to Tracking

- Inadequate policies
- Collecting keystrokes, mouse clicks, text messages, webcam photographs and screen shots, without express consent and notice
- Engaging in “history sniffing” without express consent
- Obtaining sensitive information from secured (e.g., https) webpages, without prominent notice outside of the privacy policy and terms of use advising (a) that consumer transaction data (e.g., financial credit card transactions) may be captured; (b) explaining how the information will be used or shared with third parties; and (c) obtaining express consent
- Representing that all PII was stripped from URL data through filtering technology, but in fact inadequate settings were in place to prevent disclosure of PII
- Transmitting sensitive information from secure web pages, such as financial account numbers and security codes, in clear readable text over the Internet
- Lack of a responsible senior officer
- Overriding Safari software that blocks cookies and collecting cookies from Safari users in manner inconsistent with company’s privacy representations to consumers
- Sharing persistent identifiers linked to user’s social networking profile pages (Friend Ids) with third party advertisers unaffiliated with the website publisher without notice in the privacy policy
- Inadequate encryption



Summary/Work Product/Confidential. Copyright DRS 2017



Know “Reasonable Security” – Best Practice Legal Resources

- Be aware of best practices in the form of regulatory guidance.
- California Civ. Code Section 1798.81.5 calls for “reasonable security”
- FTC’s Start With Security (2015)
- California Data Breach Report (2016)





**AGREEMENT CONTAINING
CONSENT ORDER**

FILE NO. 132 3089

The Federal Trade Commission (“Commission”) has conducted an investigation of certain acts and practices of Fandango, LLC (“Fandango” or “proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing



In re Fandango (FTC Announced Settlement March 28, 2014)

- Failure to secure mobile app credit card information.
- Alleged unreasonable security for failure to
 - Validate Secured Socket Layer (SSL) to prevent intervention by hackers when users used open networks.
 - Provide sufficient protection for data while at rest.



Regulatory Enforcement Actions – Topics Covered

- Inadequate policies
- Inadequate/improper implementation of policies
- Inadequate evaluation of security controls (whether the member is conducting, or should conduct, periodic audits to detect)
- Inadequate enhancement of controls promptly after learning of a known threat/risk
- Password-based vulnerability
- Session inactivity parameter vulnerability
- Lack of a responsible senior officer
- Inadequate steps following security incident (notification, risk assessment, etc.)
- Inadequate use of antivirus
- Inadequate use of encryption of sensitive records
- Inadequate use of application firewall
- Inadequate firewall configuration
- Lack of adequate supervision
- Inadequate training
- SQL injection vulnerability
- Failure to review incident logs
- Failure to have an IDS/IPS
- Inadequate controls over shared accounts
- Inadequate/misleading customer/consumer notification of breach
- Inadequate monitoring of vendors
- Downloading customer records by personnel onto removable media



Cal. Law Requires Vendors to Have “Reasonable Security”

CALIFORNIA DATA BREACH REPORT

FEBRUARY 2016

KAMALA D. HARRIS, ATTORNEY GENERAL
CALIFORNIA DEPARTMENT OF JUSTICE

CA AG's Feb 2016
Breach Report Says CIS
Critical Security
Controls constitutes
“reasonable security”.

California Civ. Code
Section 1798.81.5 calls
for businesses that
own, license, and/or
maintain PII to provide
reasonable security for
that information.



Tracking Disclosures and Opt-Outs



Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices

Settlement ensures consumers can control targeted ads

FOR RELEASE
December 20, 2016
TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy

Turn Inc., a Redwood City, California company that enables sellers to target digital advertisements to consumers, has agreed to settle Federal Trade Commission charges that it deceived consumers by tracking them online and through their mobile applications, even after consumers took steps to opt out of such tracking.

"Turn tracked millions of consumers online and through mobile apps even if they had taken steps to block or limit tracking," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "The FTC's order will ensure the company honors consumers' privacy choices."

According to the FTC's administrative complaint, Turn's privacy policy represented that consumers could block targeted advertising by using their web browser's settings to block or limit cookies. In fact, the complaint alleges that Turn used unique identifiers to track millions of Verizon Wireless customers, even after they blocked or deleted cookies from websites.

In addition, the agency charged that Turn's opt-out mechanism only applied to mobile browsers, and did not block tailored ads on mobile applications as the company claimed.

- Transparent disclosure of tracking activity?
- Effective opt-outs?
- Transparent disclosure of scope of opt-out?

VIZIO to Pay \$2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent

FOR RELEASE

February 6, 2017

TAGS: Telecommunications | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy

VIZIO, Inc., one of the world's largest manufacturers and sellers of internet-connected "smart" televisions, has agreed to pay \$2.2 million to settle charges by the Federal Trade Commission and the Office of the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent.

The stipulated federal court order requires VIZIO to prominently disclose and obtain affirmative express consent for its data collection and sharing practices, and prohibits misrepresentations about the privacy, security, or confidentiality of consumer information they collect. It also requires the company to delete data collected before March 1, 2016, and to implement a comprehensive data privacy program and biennial assessments of that program.

According to the agencies' complaint, starting in February 2014, VIZIO, Inc. and an affiliated company have manufactured VIZIO smart TVs that capture second-by-second information about video displayed on the smart TV, including video from consumer cable, broadband, set-top box, DVD, over-the-air broadcasts, and streaming devices.

In addition, VIZIO facilitated appending specific demographic information to the viewing data, such as sex, age, income, marital status, household size, education level, home ownership, and household value. The agencies allege VIZIO sold this information to third parties, who used it for various purposes, including targeting advertising to consumers across devices, according to the complaint.



Litigation References FTC Enforcement Actions

- *Perry v. Cable News Network, Inc.*, --- F.3d ---- (2017), 2017 WL 1505064 (Apr. 27, 2017) - Plaintiff not a consumer, and unique IDs do not specifically identify video viewing.
- *Yershov v. Gannett* 204 F.Supp.3d 353 (D. Mass. 2016) – Defendant’s motion to dismiss denied, plaintiff’s had standing to pursue the VPPA claim.
- *In Re: Vizio, Inc., Consumer Privacy Litigation*, --- F.Supp.3d ---- 2017 WL 1836366 (C.D. Cal. Mar. 2, 2017), motion to dismiss denied as to VPPA and certain other causes of action and granted in part. The FTC action had no bearing on decision. *Id.* at fn. 6.



Mitigate Privacy and Security Risks Posed by Your Vendors

Dominique Shelton



Vendor Management Checklist

Identify Which
Vendors Deal With
PII

Ensure privacy and
security terms are
in your contracts

Conduct
privacy/security
due diligence
before contracting

Monitor
compliance – post
contracting (e.g.,
SSAE 16)

Train and Engage
Your Digital Teams



Vendor Management On Your Intranet

POTENTIAL APPEARANCE OF THE VENDOR MANAGEMENT SURVEY ON AN INTRANET

A. WILL PERSONALLY IDENTIFIABLE INFORMATION BE COLLECTED?

[IF YES, CHECK BOXES BELOW AND GO TO SECTION "B" BELOW, IF NOT END SURVEY]

B. WILL THIS AGREEMENT CONCERN CREATING PROFILES OR APPENDING DATA TO CREATE USER PROFILES?

[IF YES COMPLETE DATA BROKER QUESTIONS BELOW IN NUMBER 3-4, IF "NO" GO STRAIGHT TO SECTION "C"]

C. WILL DATA PERSONALLY IDENTIFIABLE DATA BE STORED IN A CLOUD ENVIRONMENT?

[If "Yes" Go to Question 5, if "No", go straight to Section D]

D. WILL DATA BE STORED IN EUROPE OR OUTSIDE OF THE US?

[If "Yes" Go to Question 6, if "No", go straight to Section "E"]

E. WILL VENDOR AGREE TO DATA SECURITY TERMS?

[If "Yes" Go to End of Survey, if "No" go straight to Section "F"]

F. WILL VENDOR AGREE TO HELP CUSTOMER MITIGATE RISKS?



[IF YES, CHECK BOXES BELOW AND GO TO SECTION "B" BELOW. IF NOT END SURVEY]

1. If PII is at issue in this Agreement, what type?	Check all boxes that apply.	
	Apps downloaded or used	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Audio (e.g., through use of JavaScript API called navigator.getUserMedia; or browser code in HTML5 in Chrome called MediaStreamTrack.getSources() API). Read https://hdfvr.com/html5-video-recording for more information.	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Biometrics	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Calendar Information	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Call logs	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Children's Information	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Contacts/address book	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Date of Birth	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Email address	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Financial and payment information	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Cardholder data (PAN, track 1 or track 2 data)	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Geo-location (WiFi, user-entered)	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Health and medical information	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Mobile phone number	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Name	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Passwords	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Phone number	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Social Network Credentials	<input type="checkbox"/> Yes <input type="checkbox"/> No
	Text messages or email	<input type="checkbox"/> Yes <input type="checkbox"/> No
Unique Device Identifier	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Video	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Wearable sensors/activity data	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Web browsing history	<input type="checkbox"/> Yes <input type="checkbox"/> No	



Technology Governance: Assessment Sample

Data Use for OBA	
PII Protections	
Opt Out	
Opt Out Method	
Will SPI or CPNI be collected?	
If CPNI or SPI collected, list the specific elements	
Will the collected data be used for marketing purpose	
Data Joining	
Data Matching	
Data Action	
Data Record	
Data Sharing	
Vendor Use	
Vendor Contact	
Vendor Support Hours (Pacific Timezone)	
Vendor Committed Uptime	
SLA	
Scheduled Maintenance Window(s)	
Tag Failure	
Failure: Recommended Actions	
External Domains:	
Location of the Tag	
Cookie Type	
Cookie Status	
Cookie Size	
Cookie Behavior	
Comments	
Tag Code	
Tag implementation details	
Submission verification	
Status of Compliance/Privacy Review	
Status of Architectural Review	
Vendor member of NAI	
Ability to Opt out	
Ability opt out adv model	



Privacy Impact Assessment - Sample

PIA

Privacy Impact Assessment (PIA)

Privacy Office: _____
Control Number: _____
Date Received: _____

Requestor to Complete:

Vendor Risk Assessment No. if applicable: _____

SRA (Security Risk Assessment) Number: _____

Product/Service Owner's Name and Title:	(please include Employee ID)	
Phone Number:		
Project Manager's Name:	(please include Employee ID)	
Phone Number:		
Your Department:	Date of Request:	
Target Launch Date:	Full System Name:	
Has a PIA been submitted previously? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If Yes, please describe what changes and/or upgrades that are triggering the update to this PIA?		
Description of the Product/Service (Please provide a high level description of the service that a non-technical person could understand.) If needed, attach additional documentation to describe the system. Space is limited below.		
Has the new Product/Service been through a Security Risk Assessment (SRA)? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If no, please initiate an SRA (link)		

A. Will the System contain any of the following **Customer Personal identifiable Information**? ☐ Yes (Below, select all



General Data Protection Regulation

- Data Protection Impact Assessments are required if
 - (i) “high risk” to rights and freedoms,
 - (ii) profiling/automated decision-making that legally or significantly affects individuals, or
 - (iii) “large scale” sensitive data processing.



Display Advertising Ecosystem – Includes Vendors That Have PII

Ad Servers

Cross publisher ad serving with centralized creative management, campaign management, and reporting. Google Doubleclick, Atlas, Pointroll, 24/7 Real Media, Flash Talking, Mediaplex, Zedo

Data Management Platforms

Audience management consolidates audience data from various sources to help advertisers manage their audience communications and marketing programs more efficiently. Blue Kai, Krux, Lotame, X+1, Turn, Aggregate Knowledge; Adobe Audience Manager, Convento, Cross Pixel Media, Datalogix, NetSeer, Brand Screen, SocioMantic

3rd Party Data

Providers of compiled data for display audience targeting and analysis, may specialize in consumer, business, or offline-online data
exelate, Bizo, Acxiom, LiveRamp, datalogix

Advertiser / Agency

Advertiser spends on marketing to grow revenue. Agencies help them manage ad buying/creative process and budget allocation

Ford, Verizon, American Express
Omnicom, Razorfish, Publicis

Demand Side Platform (DSP)

Platform that enables media and audience buying in real time on ad exchanges (RTB global freq caps)
x+1, Turn, MediaMath, DataXu, Google Bid Manager, Criteo, Connexity

Ad Exchange

Ad Marketplace for buying and selling of ads. Publisher inventory is sold in auction to advertisers/agencies
The Trade Desk, AppNexus, BlueKai, Lotame, Nexage (Mobile), SpotXchange (Video)

Sell Side Platform (SSP)

Platform for publishers to manage yield of ad inventory, and enables routing to ad exchanges
PubMatic, Cross Pixel Media, Improve Digital, adnologies, MediaFORGE

Ad Network

Aggregator of publisher ad inventory, packaged to sell by contextual channels, audiences (BT retargeting) or buying options (CPM, CPC, CPA)
BrightRoll, Casale Media, Advertising.com, Google Display Network, AdMob (Mobile)

Publisher

Runs online business website or creates website content that generates user traffic. Ad inventory sold based on traffic volume, contextual relevancy, and audiences



In the Matter of Turn, Inc., No. 1523099 (F.T.C., Apr. 6, 2017), Docket No. C-4612

- FTC ordered conspicuous notice and opt-out for the following components of targeted advertising.
 - (a) an email address or other online contact information, such as a user name;
 - (b) a persistent identifier, such as a unique ID held in an HTTP cookie, an Internet Protocol (“IP”) address, a Device Advertising Identifier, a mobile device ID, a MAC address, processor serial number, or Verizon Wireless’s X-UIDH header;
 - (c) browsing history or other data about websites and applications that a device has accessed;
 - (d) precise geolocation data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; or
 - (e) an authentication credential such as a login ID or password



Video Vendors May Handle PII

- VPPA imposes liability for knowingly disclosing personally identifiable information defined as “information which identifies a person as having requested or obtained specific video materials or services” 18 U.S.C. §§ 2710 (a)(3); 2710(b)(1).
 - Names + video viewing; social networking ID (FB plug-ins) + video viewing. (Maiority view).





“Viewing Data” May be “Sensitive PII” According to the FTC

- Software that collects information about a selection of pixels on the screen and sends to Vizio servers where it is uniquely matched to a database of publicly available television, movie and commercial content.
- Software that also “periodically collects other information about the television, including IP address, wired and wireless MAC address, WiFi signal strength nearby WiFi access points.

Complaint, *Federal Trade Commission & Others v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. Feb. 6, 2017), Document 1 at paragraphs 14-15



Mobile App Developers Should Follow Regulatory Guidance

CA AG, FTC and EU Article 29 Working Group Guidance

PRIVACY ON THE GO

RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM

Opinion 02/2013 on apps on smart devices

January 2013

Adopted on 27 February 2013



Mobile Privacy Disclosures

Building Trust Through Transparency



Mobile App Vendors Should Build For Privacy Disclosures

Five Mobile Guides Were Released in 2013:
All Call for Just in Time/Short Form Notice

- CA AG Guidance – issued 1/10/2013
- FTC Guidance – issued 2/1/2013
- Article 29 Working Group – issued 3/2013
- NTIA Guidance – issued 7/ 2013
- DAA Guidance – issued 7/2013
- **Just in Time/Short Form Notice:** Notice for collection of sensitive data must be “Just in Time,” in short form, above and beyond the privacy policy. Ok to include in the app store.
- PII: includes unique identifiers.



Practice Pointer: Work With Your Vendors to Complete Mobile App Check List Before Launching Your App

<div><div>ALSTON & BIRD</div><div>LLP</div></div>											For Dominique Shelton, dominique.shelton@alstonbird.com David Keating, david.keating@alstonbird.com	
Appendix A Checklist												
Data types for checklist*	Check Box Yes or No	Is the data type necessary for your app's basic functionality (that is, within the reasonably expected context of the app's functions as described to users)?	Is the data type necessary for business reasons (such as billing)?	How will you use the data?	Will it be necessary to store data off the device, on your servers?	How long will you need to store the data on your servers?	Who in your organization will have access to user data?	Is your app discussed or likely to be used by children under the age of 13?	What parts of the mobile device do you have permissions to access?	Can you provide users with the ability to modify permissions?	Will you share the data with third parties (such as ad networks, analytics companies, service providers)? If so, with whom will you share it?***	How will the data be shared?
Unique Device Identifier												
Geo-location (GPS, Wi-Fi, user-entered)												
Mobile phone number												
Email address												
User's name												
Text messages or email												
Call logs												
Contacts/address book												
Financial and payment information												
Health and medical information												
Web browsing history												
Apps downloaded or used												
Videos												
Photos												
Audio												
Calendar information												
Children's information												
Passwords												
Dialer												
Microphone												
Political interests												
Biometrics												
Subject												
Identity of the Phone (e.g. John Doe's phone, as named by John Doe)												
Sexual Orientation												
Racial or Ethnic Origin												
Religious and Philosophical Beliefs												
Trade Union Membership												
Credentials												



The FTC Encourages Pre and Post Contract Vendor Security Management . *FTC Start With Security (June 2015)*

8

Make sure your service providers implement reasonable security measures.

When it comes to security, keep a watchful eye on your service providers – for example, companies you hire to process personal information collected from customers or to develop apps. Before hiring someone, be candid about your security expectations. Take reasonable steps to select providers able to implement appropriate security measures and monitor that they're meeting your requirements. FTC cases offer advice on what to consider when hiring and overseeing service providers.

Put it in writing.

Insist that appropriate security standards are part of your contracts. In *GMR Transcription*, for example, the FTC alleged that the company hired service providers to transcribe sensitive audio files, but failed to require the service provider to take reasonable security measures. As a result, the files – many containing highly confidential health-related information – were widely exposed on the internet. For starters, the business could have included contract provisions that required service providers to adopt reasonable security precautions – for example, encryption.

Verify compliance.

Security can't be a "take our word for it" thing. Including security expectations in contracts with service providers is an important first step, but it's also important to build oversight into the process. The *Upromise* case illustrates that point. There, the company hired a service provider to develop a browser toolbar. Upromise claimed that the toolbar, which collected consumers' browsing information to provide personalized offers, would use a filter to "remove any personally identifiable information" before transmission. But, according to the FTC, Upromise failed to verify that the service provider had implemented the information collection program in a manner consistent with Upromise's privacy and security policies and the terms in the contract designed to protect consumer information. As a result, the toolbar collected sensitive personal information – including financial account numbers and security codes from secure web pages – and transmitted



NIST Updated Cybersecurity Framework (Draft Version 1.1 January 2017) – Calls For Vendor/Supply Chain Risk Management

Supply Chain Risk Management (ID.SC):

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.

ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders

- COBIT 5: APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02
- ISA 62443-2-1:2009: 4.3.4.2
- ISA 62443-3-3:2013:
- ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
- NIST SP 800-53: SA-9, SA-12, PM-9

ID.SC-2: Identify, prioritize and assess suppliers and partners of critical information systems, components and services using a cyber supply chain risk assessment process

- CIS CSC:
- COBIT 5: APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03
- ISA 62443-2-1:2009: 4.2.3.1, 4.2.3.2, 4.2.3.3.
- CIS CSC:
- COBIT 5: APO10.01, APO10.02, APO10.03, APO10.04, APO10.05
- ISA 62443-2-1:2009: 4.3.2.6.4, 4.3.2.6.7
- ISA 62443-3-3:2013:
- ISO/IEC 27001:2013: A.15.1.1, A.15.1.2, A.15.1.3
- NIST SP 800-53: SA-9, SA-11, SA-12, PM-9

ID.SC-4: Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted

- CIS CSC:
- COBIT 5: APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
- ISA 62443-2-1:2009: 4.3.2.6.7
- ISA 62443-3-3:2013: SR 6.1
- ISO/IEC 27001:2013: A.15.2.1, A.15.2.2
- NIST SP 800-53: AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12

ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers

- CIS CSC: 19.7, 20.3
- COBIT 5: DSS04.04
- ISA 62443-2-1:2009: 4.3.2.5.7, 4.3.4.5.11
- ISA 62443-3-3:2013: SR 2.8, SR 3.3, SR 6.1, SR 7.3, SR 7.4
- ISO/IEC 27001:2013 A.17.1.3
- NIST SP 800-53: CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9



State AG Consent Order Against Target For \$18.5 Million – Provides Guidance For Vendor Security Management (May 15, 2017)

B. ADMINISTRATIVE SAFEGUARDS

12. TARGET shall develop, implement, and revise as necessary written, risk-based policies and procedures for auditing vendor compliance with TARGET's Information Security Program.

18. Access Control and Management:

A. TARGET shall implement and maintain appropriate risk-based controls to manage access to, and use of, TARGET's individual accounts, TARGET's service accounts, and vendor accounts, including strong passwords and password-rotation policies.

C. TARGET shall adopt a reasonable and risk-based approach to integrate two-factor authentication into TARGET's individual accounts, TARGET's administrator accounts, and vendor accounts.



Mass. Law Requires Oversight of Vendors Security Practices

- 201 CMR 17.03 “Duty to Protect and Standards for Protecting Personal Information”
- 17.03(2)(f) requires companies collecting personal information from Mass. residents to:
 - Oversee service providers, by: 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information



California – Like Another Country

- California's Confidentiality of Medical Information Act applies to software, mobile app and hardware developers.
 - It requires valid authorization before disclosure of medical information.
 - Mobile apps re: health/wellness/depression may fit this definition.
 - **Penalties \$240,000 per violation**
- California Minor Advertising Law – California minors have the right to be forgotten (similar to Europe)



Global Laws – Requiring Vendor Management

- **GDPR (effective 5/25/18)**
 - Article 44- processorObligations for onward transfer
- **Privacy Shield**
 - Contractual requirements for vendors to comply with the (1) Security and (2) Accountability for Onward Transfer Principle
- **Chinese Network Security Law (effective 6/1/17)**



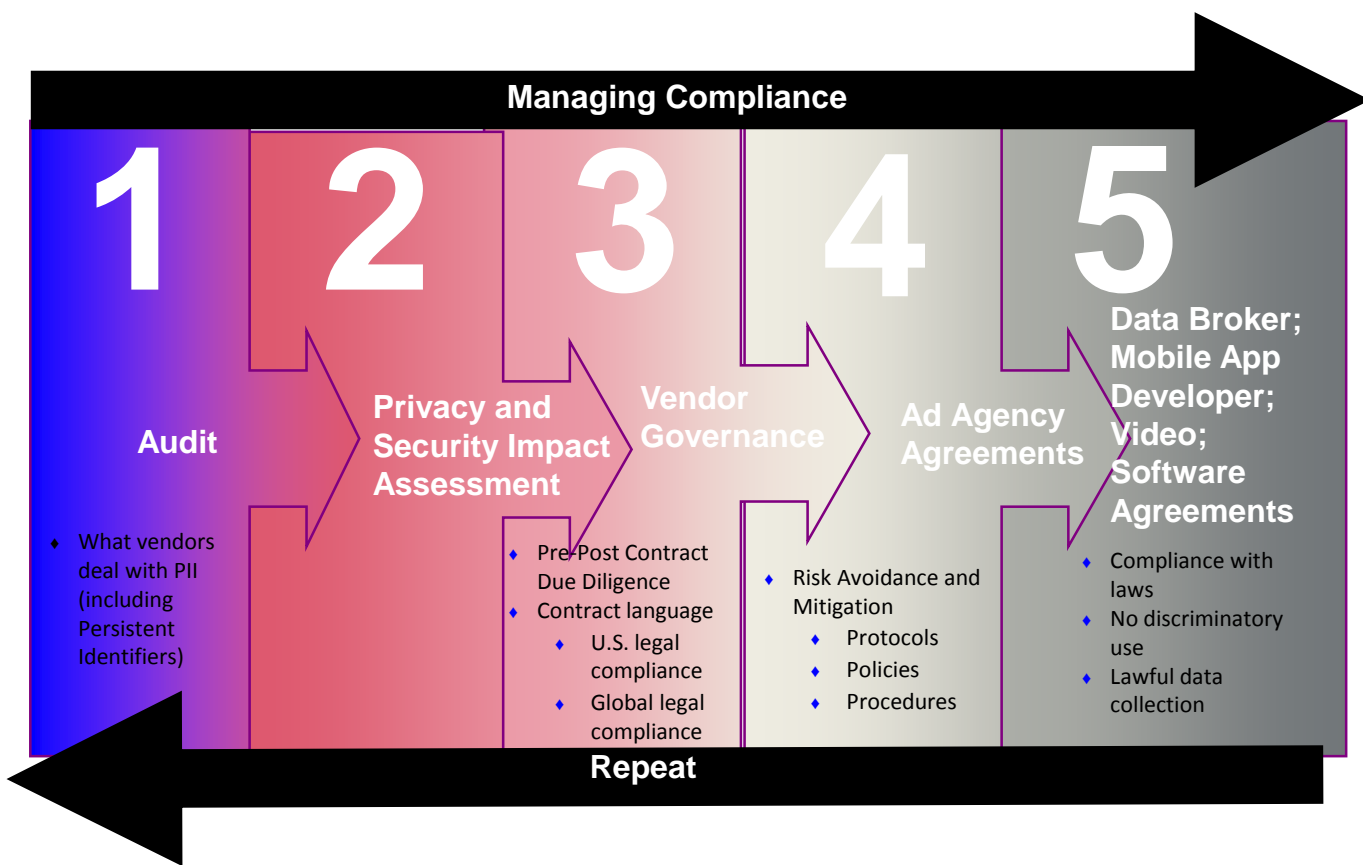


Key Contractual Provisions Include:

- Compliance with Privacy & Data Security Laws
- Privacy
 - Behavioral tracking
 - EU? Co-Controller Agreement under Article 26 General Data Protection Regulation (each controller responsible for their own tags)
 - Cross-boarder transfer
 - Mobile
 - Data minimization. Functionality of app/skills match your business needs
- Security
 - Physical, technical controls, approval of subcontractors.
 - Clouds? Ensure security is addressed.
- Insurance
 - Minimum levels.



Vendor Management Practical Guidance





Question & Thank you



Dominique Shelton

Partner, Alston & Bird

Phone: 213-576-1170

Fax: 213-576-2869

Email: dominique.shelton@alston.com