Data Privacy Considerations
When Using AI in Online Advertising
Examples of Digital Technologies

- Artificial Intelligence
- Machine Learning
- Robotic Process Automation
- Predictive Analytics
- Bots
- Business Intelligence
- Deep Learning
**Automation** refers to computer systems programmed to perform specific repetitive tasks.

**Machine Learning** refers to a computer system that has the ability to learn how to do specific tasks and/or use past data to make future decision or predictions without being explicitly programmed how to do so.

**Artificial intelligence** enables computer systems to perform the types of tasks that require human intelligence.

- Mechanizing repetitive tasks.
- Log, store, and produce reports
- System that monitors transactions.
- Scans transactions for patterns
- Improve over time from analysis of the “training data”
- Deep learning is a type of Machine Learning
- Obtain knowledge by finding patterns in raw data
- System that analyzes huge volumes of conversations from data pools and leverages algorithms to determine behavior.
- Contextual analysis and building generalizations to inform decisions
- Algorithms can be optimized, but can fail like human knowledge
What is AI?

Technology that can *perceive, learn, reason, assist in decision-making, and act* to help us solve problems.
Values AI needs to respect

- Fairness
- Reliability & Safety
- Privacy & Security
- Inclusiveness
- Transparency
- Accountability
Current Applications

- Online recommenders
- Chatbots (Cortana, Alexa, online “customer service”)
- Facial/body recognition
- Blockchain technology
- Autonomous vehicles/drones
- Gaming
- Medical decision support systems
- Hearing aids
- Robotic pets and cleaning robots
AI in Advertising

• Online behavioral tracking
• Social media/web scraping

Source: Hasbro Industries, Inc.
Online Behavioral Tracking

Source: Disney Enterprises, Inc.
FTC Online Behavioral Advertising

• Principles issued in 2009:
  – Transparency and Control
  – Reasonable Security and Limited Data Retention
  – Affirmative Express Consent for New Use
  – Affirmative Consent Prior to Collection of Sensitive Data

FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (2009)
FTC Guidance on Cross-Device Tracking

• Transparency
• Choice
• Avoid cross-tracking sensitive topics (e.g., health, financial, and children’s information)
• Have and maintain reasonable security

FTC Staff Report (Jan. 2017)
Other Resources

• Digital Advertising Alliance (“DAA”) Cross-Device Guidance (Nov. 2015)
  – Effective February 2017:
    • Consumer’s opt-out on one device to prevent that device from receiving behavioral ads will prevent data from that device from informing behavior ads on other devices

• Network Advertising Initiative (“NAI”) Cross-Device Linking (May 2017)
Social Media/Web Scraping

Source: Comedy Partners, Composed of Viacom International Inc. and Viacom Hearty Ha! HA! LLC
Social Media and Web Scraping

• What is “web scraping”?  
  – Web scraping is the targeted capture of information from websites  
  – Early variants included crawlers for indexing, price comparison, and reviews  
  – Not new, but the consequences have evolved  

• In the social media contexts, web scraping has greater consequences  
  – Concerns for privacy, intellectual property, and terms of use
Facebook Privacy Controversy

Cambridge Analytica
Facebook Privacy Controversy

• Last month, the FTC confirmed it opened investigations into possible privacy violations at Facebook related to Facebook’s 2012 settlement order with the FTC
• The case stemmed from Cambridge Analytica’s purchase of personal data
• Massive questions about Facebook’s actions, but also about the future direction of privacy in social networking
• Directly implicates targeting advertising and messaging
Facebook Privacy Controversy

• Facebook business model
  – Primarily focused on advertised based business
  – Ad profiles based on user activity
  – Interaction-based and network-based
  – Relationship between contacts can elaborate ad profiles
  – Privacy approach is robust but defaults are relatively open

• 2012 FTC Order
  – Terms of order focused on (i) representations to users about security, (ii) representations to users about data collection, and (iii) availability of information to third-parties
Facebook Privacy Controversy

• Social networks depend on capturing data and analyzing users
Facebook Privacy Controversy

- Social networks depend on capturing data and analyzing users
Facebook Privacy Controversy

• User data policies:
  – Data storage policies
    • Onsite data
    • Offsite data
  – Data collection policies
  – Data sharing with third-parties
  – Data use
  – Profiling
Facebook Privacy Controversy

• Cambridge Analytica’s actions and model
  – Cambridge Analytica sought data sources to create targeted advertisements aimed at certain voters in the US and abroad
  – Cambridge Analytica bought its data as a mini-warehouse rather than directly soliciting the data from users

• Data warehouse acquisition is not unusual
  – Acquired data from “This is Your Digital Life” app
  – Facebook alleges Cambridge Analytica misused this data in violation of Facebook terms of service
Facebook Privacy Controversy

- Cambridge Analytica profiling
Facebook Privacy Controversy

• FTC Commentary on Investigation
  – What is driving the investigation?
  – Key concerns from FTC

• International regulatory reaction

• Facebook response

• Industry response
Takeaways

• What precautions should companies take when using third-party data that may have been scraped?
  – Legal risks to advertisers
  – Legal risks to parties using analytics
  – Implications for GDPR
• Reconciling US legal concepts with international concepts
• What kinds of scraping/mining are safe, and what are clearly problematic?
Legislation

General Data Protection Regulation (GDPR)

• Effective May 25, 2018
• Applies to:
  The processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the Union, where the processing activities are related to:
  a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
“Personal Data”

- Means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
“Processing”

- Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
“Consent”

• Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Some Data Subject Rights

• Right to erasure/right to be forgotten (Article 17)
• Data portability (Article 20)
• Right not to be subject to automated decision-making (Article 21 and 22)
Right to Object

- Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
Automated Decision-Making

• The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
“Profiling”

• Means any form of **automated processing of personal data** consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, **behaviour**, location or movements
Automated Decision-Making (cont.)

• Exclusion: If automated decision “is based on the data subject’s explicit consent.”

• Notwithstanding the exclusions, automated decisions should not be made on “special categories.”
  • Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Controller Obligations

• Tell data subject about existence of automated decision-making, provide meaningful information about logic involved, and significance and consequences of such processing
• Inform data subject if processing data for other purposes other than for which it was collected
• Implement procedures for data subject to obtain human intervention, express POV, and contest decision
What if…

• You have a website
• You do not target EU citizens
• You use cookies and other tracking devices
• What do you do?
Recital 23 – Offering of Goods/Services

• In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
Recital 24 – Monitoring of Behavior

In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
California Legislation – AB 1950

• Introduced on January 29, 2018
• Requires social media sites to identify and verify with a disclaimer all bot accounts
• Requires bots to be linked to a verified human and that all advertising purchases on social media be made by verified human accounts
Better Online Ticket Sales Act ("BOTS Act")

- Makes it illegal to “circumvent a security measure, access control system, or other technological control or measure on an Internet website or online service used by the ticket issuer to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing rules.”

  15 U.S.C. § 45c
  Enacted Dec. 14, 2016

- Sound like something?
Possible Cause of Action

- DMCA, 17 U.S.C. § 1201(a): “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”
CLOUD Act

• Clarifying Lawful Overseas Use of Data Act

• Signed into law on March 23, 2018

• To provide law enforcement access to data stored outside the US and held by communications-service providers, who are subject to US jurisdiction

• Creates a framework for resolving conflicting legal obligations by providing a mechanism for bilateral agreements that govern cross-border investigative demands
CLOUD Act (continued)

- Bilateral Agreements
- Extraterritoriality of US Warrants and International Comity
- Transparency
- Reciprocity
A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider’s possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States. 18 U.S.C. § 2713 (as amended).
CLOUD Act (continued)

• Provides executive branch the ability to enter into “executive agreements” with foreign nations to allow each nation to obtain user data stored in the other country—regardless of the nation’s privacy laws and without congressional approval
Some Best Practices
Best Practices

• All about the Data!

• Understand how the technology works and business impact

• Review advertising materials and methods, including social media platforms

• Review and update privacy policies

• Review and update vendor agreements

• IT, Marketing, Company should communicate
Thank You

Source: Lucasfilm