

BakerHostetler



## The Latest in Big Data and Cyber Security Contracts

Presented by: Melinda McLellan

*December 11, 2017*



**Melinda L. McLellan, Partner**  
mmclellan@bakerlaw.com  
212.589.4679

# Agenda

- IP and Data Ownership + Usage Restrictions
  - Confidentiality, Trade Secrets, De-identification
- Privacy and Data Security
  - Privacy Law Overview
  - FTC Regulation of the IoT, Best Practices
  - IoT Enforcement Actions and Lawsuits
- Vendor Agreements
  - Key Contract Terms to Consider
  - Negotiation Strategies

# IP and Data Ownership and Usage Restrictions



# Development of New IT/IP, Licensing of Third Party IP and EULA

BakerHostetler

- Device (design and IT)
- Mobile Apps
- User Interface
- Access and Use of Platforms and SDKs
  - E.g., Arrayent, Nest, Google, Apple, Alexa
- E-Commerce partners (e.g., Febreze refills, Oral B brush replacements)
  - Amazon
- Backend and ancillary operations
- End User License Agreements and Privacy Policies

# Consider Data Types & Classification

- Types of data
  - Data provided by or for customers
  - Data resulting from vendor's processing of customer data
  - Usage data
- Information classification
  - Confidential
  - Trade Secrets
  - Personally Identifiable Information
  - Sensitive Personal Information
  - Protected Health Information
  - Payment Card Information

# Vendor Data Usage Considerations

- Data includes
  - Raw data points
  - Database
  - Analytic tools
  - Output / analysis
- Data inputs vs. outputs
- Vendors may use data
  - To perform the services for client
  - To operate or improve vendor's own services
  - To create vendor derivatives (analytics, market intel, etc.)

# Avenues of Protection

- License
  - Ability to restrict access to raw data = licensing opportunities
- Trade Secret
  - Data that can be kept from the public domain
- Copyright
  - Databases and reports
- Patent
  - Sensors, networking, and pathways



# IP Considerations Regarding Data

- Is there copyright in the raw data?
- What rights in the databases?
- Who owns the tools used to analyze the data?
- Who owns the analytic reports?
- Who owns the insights gained from the reports?



# Data De-Identification / De-Linking

## A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION



What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



This is a primer on how to distinguish different categories of data.

### DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

### PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.



### DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.



### ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

- DIRECT IDENTIFIERS**  
Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)
- INDIRECT IDENTIFIERS**  
Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)
- SAFEGUARDS and CONTROLS**  
Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals

	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
<b>IDENTIFIERS</b>	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>INDIRECT IDENTIFIERS</b>	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
<b>SAFEGUARDS and CONTROLS</b>	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation

#### SELECTED EXAMPLES

Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)

Unique device ID, license plate, medical record number (e.g., MAC address 08:00:00:33:00:03)

Same as Potentially identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses to legal representations)

Clinical or research datasets where only curator retains key (e.g., Jane Smith, diabetes, Hgb 15.1, gID = Cark23)

Unique, artificial pseudonyms replace direct identifiers (e.g., HPIA Limited Datasets, John Doe = 3177 LK6952) (unique sequence not used anywhere else)

Same as Pseudonymous, except data are also protected by safeguards and controls

Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPIC: 3.2 = 3.0-3.3, gender: female = gender: male)

Same as De-identified, except data are also protected by safeguards and controls

For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)

Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)

# Data Privacy and Security Requirements and Breach Notification



“ongoing forensic investigation has indicated that the intruder stole a vendor’s credentials which were used to access our system”

- Molly Snyder, Target spokeswoman

Source: Wall Street Journal, *Target Hackers Use Stolen Vendor Credentials* (January 29, 2014)

# The Privacy Law “Patchwork”

- Federal & state laws govern the handling of personal information
  - GLBA/HIPAA/FCRA/COPPA/DPPA/VPPA/ECPA/SCA
  - Laws protecting SSNs / disposal of PII
  - Employment-related privacy laws
  - FTC Act enforcement
  - Marketing privacy issues (TCPA, CAN-SPAM, CASL...)
  - State-specific (e.g., IL BIPA, MA Regs, NYDFS, CA “RTBF”)
- State breach notification laws
- Industry standards and guidance
- International data protection regulations

# Federal Trade Commission

- Section 5 Enforcement Authority
  - Concerns “unfair” and “deceptive” trade practices
  - FTC: de facto privacy law regulator in the U.S.
- Consumer data protection in many contexts
  - Sale of data (e.g., in bankruptcy, M&A)
  - Misleading claims about online tracking
  - Cross-device tracking concerns
  - Recently: increased interest in the Internet of Things
- The FTC enforces a variety of consumer protection statutes (e.g., FCRA, COPPA, Do-Not-Call, FACTA, CAN-SPAM) that prohibit specifically-defined trade practices

# IoT: FTC and NTIA = P-b-D

## FTC's recommended best practices:

- Build privacy and security into devices and software at the outset
- Train employees on good practices
- Ensure downstream privacy & data protections via vendor contracts and oversight
- Apply defense-in-depth strategies that offer protections at multiple levels and interfaces
- Employ reasonable access controls
- Limit the amount of data collected/retained
- Securely dispose of data when no longer needed
- Where practicable, provide info to allow consumers to decide if and how their data will be collected and used

# Enforcement & Litigation

BakerHostetler

- TRENDnet, FTC Settlement (9/13)
- Aaron's Rent-to-Own, FTC Settlement (10/13)
- Hello Barbie, Class Action Filed (12/15)
- D-Link, FTC suit (filed 1/17)
- VIZIO, FTC/NJ joint enforcement (2/17)
- We Vibe, Class Action Settled (3/17 - \$3.75m)
- Advocacy Groups Challenge Children's Smartwatches (10/18)

# Data Protection Management

- Conduct privacy and security due diligence when developing tech, selecting vendors and throughout commercial operations
- Ensure each third party agreement contains appropriate protections
- Monitor vendors and other third parties to verify that they comply with their privacy and security obligations throughout the life of the relationship



# Key Agreement Data Protection Terms

- Appropriate administrative, technical, and physical safeguards to protect data and comply with all applicable laws (specify for certain industries)
- Definitions (“Personal Information” “Information Security Incident”)
- Employee training and enforcement of policies
- Notification of potential and actual incidents; government requests
- Indemnification/Limitations of Liability/Cyber Insurance
- Restrict further use or disclosure of company data by vendor (other than what is necessary to perform the services)
- Impose requirements concerning data retention, and destruction (or return of all data) at termination of the agreement

# Dealing with Vendor Pushback

- Use the law for leverage
  - Especially if a regulated industry
- If the vendor resists, seek quotes from other vendors (include in RFP process)
- If they all resist, document the problem to improve defensibility (evidence of “reasonableness”) including:
  - Due diligence protocol
  - Attempts to locate alternate/cooperative sources

# BakerHostetler

Atlanta  
Chicago  
Cincinnati  
Cleveland  
Columbus  
Costa Mesa  
Denver  
Houston  
Los Angeles  
New York  
Orlando  
Philadelphia  
Seattle  
Washington, DC

[www.bakerlaw.com](http://www.bakerlaw.com)