Top Four (or maybe Five) Marketing Privacy Issues for 2018

Association of Corporate Counsel
November 2, 2017

Tanya Forsheit, Co-Chair Privacy & Data Security Group, Frankfurt Kurnit Klein & Selz
Kendra Litner, Assistant General Counsel, Deloitte
Deirdre J. Sheridan, Director & Senior Counsel, Privacy Officer, New Avon LLC
Agenda

• How Can I Possibly Be Ready for the EU General Data Protection Regulation (GDPR)?
• What Exactly is Happening on All Those Websites and Apps?
• Incident Response in 2018—I Get the PII Stuff, But How Do I Protect the Company’s Crown Jewels?
• Internet of Things --- Home Assistants, Wearable Tech, and Connected Cars, oh My!
• The Enforcement Picture --- What's Next for the FTC and State Attorneys General?
GDPR – How Can I Possibly Be Ready?

HELP!!!!
Where to Start?

• Determine If You Are a Data Controller or Data Processor, or Both
• Appoint a Data Protection Officer (DPO)
• Prepare Personal Data Inventories for Consumer and HR Personal Data
Where to Start? (cont.)

• Identify Legal Bases for Data Processing
  • Consent
  • Legitimate Interest
  • Contractual Necessity
  • Other Lawful Grounds
  • Special Categories
• Implement Privacy by Design and by Default
• Pseudonymize? Yes
Where to Start? (cont.)

- Attention to Vendor Agreements
- Establish Procedures for Handling Data Subject Requests to Exercise Rights
  - Transparency
  - Access
  - Rectification
  - Erasure
  - Right to Be Forgotten
  - Restrict Processing
  - Object
  - Data Portability
  - Data Profiling Rights
- Implement Appropriate Data Security Measures and Prepare, Maintain and Test Incident Response Plan

Copyright: <a href='https://www.123rf.com/profile_nonwarit'>nonwarit / 123RF Stock Photo</a>
Where to Start? (cont.)

- Conduct Data Protection Impact Assessments (DPIA)
- Review and Revise Privacy Notices
- Make Sure Your Data Transfer Mechanisms Are Lawful
- Train Your Personnel
- Maintain Appropriate Documentation
Why do we care? Enforcement

- Member State Courts and DPAs
- Administrative fines up to
  - 20 million EUR; or
  - 4% of the total worldwide annual turnover of the preceding fiscal year,
... whichever is higher
What Exactly is Happening on All Those Websites and Apps?
Tracking Technologies

• Cookies, beacons, embedded scripts, location-identification technologies (more on that to come), device fingerprinting, in app-tracking methods, etc.

• Analytics, interest-based advertising, social media
Online Behavioral Advertising

- Not new
- FTC definition in 2009 - the tracking of a consumer’s online activities over time – including the searches the consumer has conducted, the web pages visited, and the content viewed – in order to deliver advertising targeted to the individual consumer’s interests.
Legal Requirements

• California disclosures– CalOPPA
• Privacy Policies
• Do Not Track disclosure
• EU ePrivacy Directive
• Cookie Policy
• Forthcoming EU ePrivacy Regulation – application more expansive
FTC 2009 Guidance and Principles

• Transparency and consumer control
• Reasonable security, and limited data retention, for consumer data.
• Affirmative express consent for material changes to existing privacy promises.
• Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.
Recommendations:
• Be transparent
• Give consumers choices
• Don’t engage in cross-device tracking with respect to sensitive data
• Limit data collection to what necessary and delete it when no longer needed
Self-Regulatory

• Self-Regulatory: American Association of Advertising Agencies (AAAA), the Association of National Advertisers (ANA), the Direct Marketing Association (DMA), and the Interactive Advertising Bureau (IAB), and supported by the Council of Better Business Bureaus (BBB)

• NAI and DAA AdChoices
In Practice?

• What do privacy policies say about first and third party tracking technologies?
• What kind of just-in-time notices are provided if any?
• How are choices made available to the user?
• What do contracts say about allocation of responsibility?
Collection of Precise Geolocation Data

• Do not collect or share precise geolocation data without obtaining affirmative opt-in consent.

• Usually facilitated through push via app platform.
BOTTOM LINE - DON’T BE CREEPY

• NO STEALTH TRACKING

• NO ZOMBIE COOKIES
Incident Response – How to Avoid a Nightmare

See, e.g., Equifax . . .
After an Incident – 1st and Foremost

KEEP CALM AND PLAY IT COOL
Data Breach Notification Laws

• Beginning in 2002, legislators across the country began passing laws requiring consumer notification when there is a security breach involving private information.

• Forty-eight states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have passed security breach notification laws affecting private entities.

• Most follow California’s lead, but with some key differences (e.g., “material” breach requirement; expanded definition of “personal information”; breach involving non-computerized data; notification procedures; requirement to notify consumer reporting and/or law enforcement agencies; exemptions from mandatory notification (e.g., encryption); penalties)
Practice, Practice, Practice

• While data breaches are inevitable, the company can take measures to be ready for the next breach.
• The Team
  – Internal Stakeholders
  – External Vendors
    • Legal
    • Forensics
    • Mailing and Call Center
    • Remediation
    • Crisis Communications
• The Incident Response Plan
• Drills/Tabletop Exercises
Investigate, Contain & Respond

- Investigate!
- Contain!
- Notify (as applicable and pursuant to statute):
  - Internal Stakeholders and affected Business Partners/Vendors
  - Affected Individuals
  - Regulators
  - Card companies
  - Law enforcement
  - Auditors
  - Others?
- Remediation Services?
- Communications Strategy?
Internet of Things
The Internet of Everything

• February 6, 2017, FTC and NJ AG settlement with Vizio Inc. $1.5 million to the FTC and $1 million to NJ – alleged collection of information about consumers’ video viewing behavior and sharing without sufficient notice or consent. Similar pending class action litigation against Vizio.

• Class actions ongoing.
IoT

• Alexa – what kind of evidence do you have for me in this criminal investigation?

• Fitness trackers: MLB approval of wearable tech on the field

• Connected Cars: industry action; Congressional scrutiny
The Enforcement Picture – FTC and State AGs
FTC – A Few of the Latest and Greatest

• December 20, 2016: Deceptive Tracking. Settlement with digital marketing platform Turn Inc. over claims that the company deceptively tracked users across the Internet for advertising purposes.

• July 5, 2017: False Promises. Settlement with Blue Global Media, LLC and its CEO over allegations that the company solicited consumers to provide sensitive information based on false pretenses and then shared that information with potential buyers without any regard for the protection or security of that information.

• September 8, 2017: Failure to Certify. Settlement with 3 companies for allegedly making false statements in their privacy policies that they participated in Privacy Shield when they had not actually registered as participants with the Department of Commerce.
State AGs at the Door

- **Vermont: Failure to Report!** Assessed fine of $264K for exposure of Social Security numbers of only 660 people because an affected citizen, not the company itself, reported the breach.

- **New York: Be Transparent.** Fitness apps Cardiio, Runtastic and My Baby’s Beat agreed to pay a combined $30,000 in fines and revise their advertising claims and privacy policy disclosures. Among other things, the apps were not clear how user data could be shared with third parties.