Navigating Privacy "Must Haves" and "Should Haves" in the Mobile App Environment

November 30, 2015

Reed Freeman

Heather Zachary

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Reed Freeman
Partner
WilmerHale

Heather Zachary
Partner
WilmerHale

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and 1.0 non-transitional CLE credit in New York*
- WebEx customer support: +1 888 447 1119, press 2

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.*

Overview

- FTC's Expectations for Mobile Privacy and Security
- FCC and State Law
- Filling the Gaps with Self-Regulatory Guidance
- Lessons from the Telephone Consumer Protection Act
- Key Differences in Canada, the EU, and APEC
- Mobile App "Must Haves" and "Should Haves"
- Questions

FTC Expectations for Mobile Privacy and Security

Privacy Disclosures in the Mobile Context

The FTC has acknowledged that mobile devices present unique challenges for privacy and the need to provide clear, conspicuous, and effective disclosures.

- 2012 FTC report ***Protecting Consumer Privacy in an Era of Rapid Change*** raised special concerns about the constant data flow and limited disclosure space in mobile devices.
- 2013 FTC report ***Mobile Privacy Disclosures: Building Trust Through Transparency*** provided specific guidance for players in the mobile ecosystem: platforms, app developers, third parties, and trade associations.
  - Implement "just-in-time" notice to obtain express consent prior to collecting sensitive information such as precise location, contacts, photos, etc.
  - Develop privacy dashboards and icons (e.g., icon when location tracking in use)
  - Link to privacy policies in app store, prior to download
  - Coordinate and communicate among app developers and third parties
  - Implement DNT mechanism for smartphone users
- 2013 FTC guidance ***.com Disclosures*** provided advice about how to make effective disclosures in digital advertising.

FTC's Privacy Expectations: Representations Must be Accurate and Complete

The FTC has brought numerous cases alleging falsity of promises that mobile app companies have made to consumers about their data.

- **Nomi**: Retail mobile location-tracking service misled consumers with promises that it would provide an in-store mechanism for consumers to opt out. Violation found even though promises went beyond what the law required.
- **Brightest Flashlight**: Mobile app claimed to collect information purely for internal housekeeping purposes, then sold it to third-party advertisers.
- **Path**: Collected personal data from users' mobile device address books, contrary to statements in privacy policy.
- **Snapchat**: Claimed that real-time "snaps" would "disappear forever" despite recipients' ability to save messages indefinitely via third-party apps.

FTC Expectations: Data Security

The FTC Standard: Administrative, technical, and physical controls to protect against reasonably foreseeable threats to the security, confidentiality, and integrity of consumers' personal information, taking into account the size and complexity of the company, the nature of its activities, and the sensitivity of the data.

Recent Mobile Data Security Cases

- **Fandango / Credit Karma:** allegedly disabled default SSL certificate validation on mobile apps, leading to potential vulnerabilities of "man-in-the-middle attacks"—no breach or loss of personal information alleged
- **HTC America:** design flaws in mobile device software allegedly allowed third-parties to bypass Android's permission-based security model
- **Snapchat:** allegedly failed to secure its "Find Friends" feature, which allowed attackers to compile a database of 4.6 million usernames and phone numbers

FCC and State Law

Federal Communications Commission

- Federal Communications Commission rules govern the privacy and security of consumer information.
  - The FCC has long policed the privacy and security of consumer information through Section 222 of the Communications Act and its Customer Proprietary Network Information (or "CPNI") rules.
- The FCC's recent expansion of authority to cover broadband providers raised the question of whether "edge providers" (such as Google, Facebook, Pandora, and Netflix) would be subject to FCC jurisdiction.
  - In its March 2015 "Open Internet" Order, the FCC stated that it was ***not "regulating the Internet, per se, or any Internet applications or content."***
  - Similarly, on November 6, 2015, the FCC dismissed a petition to require "edge providers" to honor DNT requests: ***"The Commission has been unequivocal in declaring that it has no intent to regulate edge providers."***
- Nonetheless, mobile apps may be regulated by the FCC in some contexts, such as in relation to VoIP services or when common carriers collect information through mobile apps.

Federal Communications Commission

- FCC enforcement has been aggressive and potentially could reach other conduct.
- The FCC announced in April 2015 that it was investigating common carriers' practices of adding header information to wireless network traffic for device identification purposes.
  - Consumer privacy advocates raised concerns about the manner in which third parties could use the information for tracking purposes.
  - The FCC stated that its investigation related in part to "the collection and use of information about their subscribers' Internet activity."
- The FCC's enforcement bureau recently hired a well-known privacy advocate/technologist with a background in online, mobile, and retail tracking technologies.
  - More enforcement to come?

California Online Privacy Protection Act

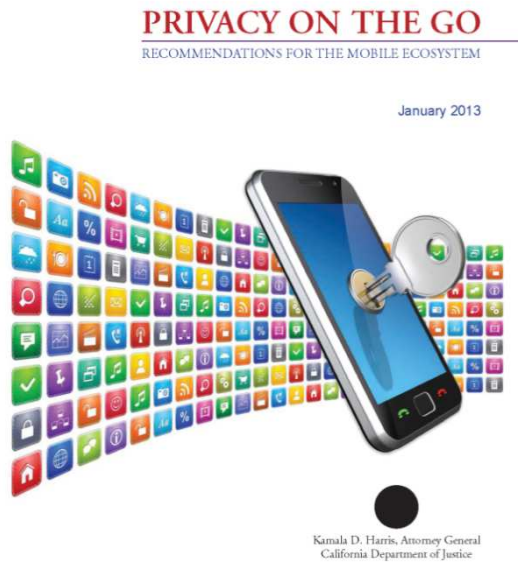
The California Online Privacy Protection Act (CalOPPA) applies to Web sites and "online services."
See Cal. Bus. & Prof. Code §§ 22575 *et seq.*

- The Attorney General has stated that a mobile application is one type of online service
- CalOPPA's recent amendments have unique implications for apps. For example, companies must make the privacy policy available through "reasonably accessible means" and disclose:
  - Whether other parties may collect information about users' "online activities over time and across different *Web sites*"
    - Does this include cross-app advertising?
  - How the operator responds to browser 'do not track' signals or similar mechanisms
    - E.g., "Limit Ad Tracking" features in iOS or Android
  - How registered users under age 18 can remove content posted to mobile apps
- The California AG has sued to enforce CalOPPA as applied to mobile apps—for example, Delta's app collected PII but did not have a privacy policy.

California's Mobile Privacy Recommendations

In 2013, California issued a report with mobile privacy recommendations for app developers, app platform providers (*e.g.*, app stores), advertising networks, and others:

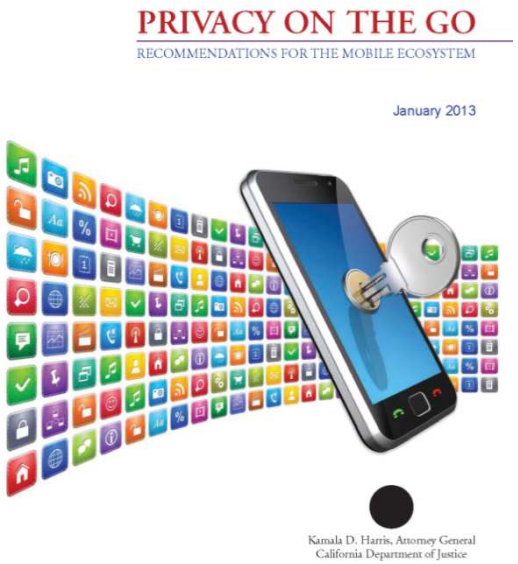
- Make your privacy policy accessible from within the app (e.g., through the "About" or settings page) and in the app store so users can read it before they download
- Use shorter privacy disclosures and other measures to draw attention to data practices that may be unexpected
- Enable meaningful choices about the collection and use of data
- Augment disclosures when collecting sensitive data, text messages, call logs, contacts, or using sensitive device features (e.g., cameras, microphones, location tracking)



California's Mobile Privacy Recommendations

Practices to <u>avoid</u>:

- Collecting personally identifiable data that is not necessary for the functions of the app
- Using out-of-app ads delivered by modifying browser settings or placing icons on the mobile desktop
- Using static, device-specific identifiers for advertising (e.g., MAC address or IMEI)



See Privacy on the Go: Recommendations for the Mobile Ecosystem
http://www.oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf?
See also Making Your Practices Public: Recommendations on Developing a Meaningful Privacy Policy
https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

Filling the Gaps with Self-Regulatory Guidance

Self-Regulation of Interest-Based Advertising (IBA)

The Digital Advertising Alliance (DAA) *Self-Regulatory Principles for Online Behavioral Advertising* and subsequent guidance relate to the use of information collected over time and across unaffiliated web sites, apps, and devices

- **Transparency**
  - First parties must disclose third-party IBA practices
  - Third parties must disclose: (1) types of data collected for IBA; (2) uses/transfers of data; (3) opt-out; and (4) adherence to DAA Principles
  - "Enhanced notice" required in or around interest-based ads and/or on web pages or apps where data is collected or used for IBA

- **Consumer Control/Choices**
  - Opt-out required for IBA
  - Opt-in required for sensitive health or financial data, material changes to existing policies, or collection/use of data by "Service Providers"
- **Data Security and Accountability**
- **Prohibitions on use of multi-site data for employment, credit, health, and insurance eligibility**

Self-Regulation of Interest-Based Advertising (IBA)

The Network Advertising Initiative (NAI) adopted its first self-regulatory code of conduct in 2000

- The ***2015 NAI Code of Conduct*** contains requirements similar to the DAA's Self-Regulatory Principles, but members also must disclose:
  - Ad delivery/reporting practices;
  - Technologies used;
  - Data retention period;
  - Adherence to NAI Code; and
  - Use of health-related interest segments

- Members must require by contract that first parties disclose IBA practices/opt-out and make "reasonable efforts" to confirm that first parties comply with such requirements
- Restrictions on merger of PII with non-PII and transfers to third parties
- Additional requirements for data access, quality, security, and retention

DAA and NAI Mobile Guidance

In 2013, the DAA and NAI each released ***mobile guidance*** to apply existing principles in the mobile context

- Covers tracking in mobile applications
  - Introduced the concept of "cross-app data," defined by the DAA as ***data collected from a particular device regarding application use over time and across non-Affiliate applications***
  - Requires enhanced notice for advertising based on cross-app data, which could include notice through app stores, installation process, or app settings
- Requires ***consent*** for the collection and use of:
  - Precise location data; and
  - Personal directory data (e.g., contacts or address book)
- Some differences in terms of what to include in notice and other nuances
- ***"AppChoices" tool*** launched in February 2015 for opt out in mobile apps
- Enforcement of DAA Principles in mobile environment began September 2015

NAI Guidance on Precise Location

Section I.G of the NAI Code of Conduct defines ***Precise Location Data***:

- "[I]nformation that describes the precise geographic location of a device derived through any technology that is capable of determining with reasonable specificity the actual physical location of a person or device, such as GPS level latitude-longitude coordinates or location."
- Excludes data that is or will be altered
- Excludes contextual uses (e.g., to deliver advertisements in real time without storing)

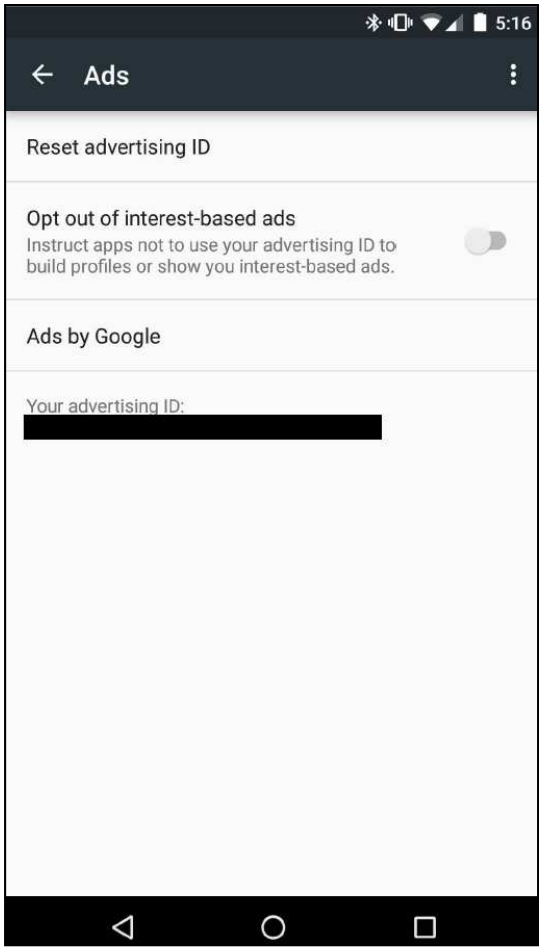
In July 2015, NAI released *Guidance for NAI Members: Determining Whether Location is Imprecise* to clarify the conditions under which location data is considered ***"de facto" imprecise***:

- Lat/Long coordinates with ***two or fewer decimal places***
- Geographic equivalent, e.g. ***area of a circle with a radius of greater than 500m***
- Same standard applies to specific locations (e.g., Disney World, Central Park, San Francisco, or "Starbucks")
- Four-factor analysis for close cases: area, population density, accuracy, time

Beyond Cookies: Tracking with Client IDs

Examples:

- **HTML5 local storage**
  - Similar to cookies
- **Flash cookies**
  - Similar to HTTP cookies, but controversial and works across browsers
- **Platform IDs (Android and iOS)**
  - Apple and Google have strict limitations on how their advertising identifiers can be used
  - Device specific, like the Statistical ID
  - Works across multiple apps and programs on a single device or operating system, but depending on the client ID implementation, may only be available through native applications and not through a mobile browser, for instance, as is the case with the Apple advertising identifier



Mobile Platform Identifier Terms

Android, iOS, and Windows phones have platform advertising identifiers

- User control: opt-out or reset the identifier

Android and iOS are very similar in their terms. For both:

- Must use for advertising
  - Cannot use any other identifiers for advertising w/o opt-in consent
  - Android identifier "must not be connected to personally-identifiable information or associated with any persistent device identifier (for example: SSAID, MAC address, IMEI, etc.) without the explicit consent of the user."
- Must honor the opt-out
  - Cease interest-based advertising only
  - Do not have to cease contextual advertising, ad delivery and reporting, frequency capping, security and fraud prevention, etc.
- Must honor the reset
  - Cannot connect current ad ID to previous ad ID
- Use of the identifier must be disclosed in the privacy policy

Beyond Cookies: Tracking with Statistical IDs

What is a Stat-ID?

- Uses the unique characteristics of your browser/device to maintain state (e.g., IP address, user-agent string, plug-ins, fonts, exact browser version)
- Been around for a number of years, but, until recently, more commonly used for fraud detection than tracking for advertising purposes
- Device-specific, but can work across multiple apps or programs on a single device

Cannot fully replace the cookie because not sufficiently persistent

- IDs may change frequently as the device changes
- A truly stable and persistent statistical ID that would be sufficient for maintaining a shopping cart or honoring consumer privacy preferences (for instance), would be difficult to maintain

Issues with transparency

- No storage on the user's computer, so very hard to detect that it is happening

NAI Guidance on Non-Cookie Technologies

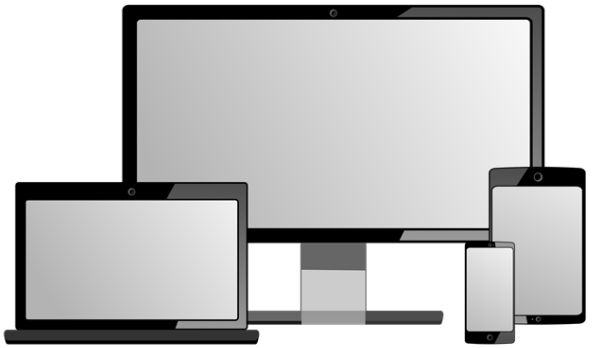
In May 2015, NAI released *Guidance for NAI Members: Use of Non-Cookie Technologies for Interest-Based Advertising Consistent with the NAI Code of Conduct*

- **Transparency and Notice Requirements**
  - Describe use of non-cookie technologies and applicable opt-out
  - Describe and link to consumer transparency tool
  - Update any representation that browser cookie controls alone will halt all interest-based advertising
  - Update other disclosures as required (e.g., data collected or data retention)
  - Ensure first-party notice
- **Control Tools**
  - Implement opt-out tool on website and NAI opt-out page
  - New opt-out tool in development: will use combination of third-party cookies, first-party cookies, and/or alternative technologies as approved by the NAI
  - For technologies without consumer-facing browser controls (e.g., stat ID), must offer the ability to stop prospective data collection or disassociate previously collected data from browser
- *See also* the ***Online Interest-Based Advertising Accountability Program's Compliance Warning*** clarifying that DAA Principles apply irrespective of technology used

Cross-Device Linking: Overview

What is cross-device linking?

- Infer connections among various browsers or devices (e.g., tablets, smartphones, web browsers, as well as other internet-connected devices such as TVs or game consoles)
- Multiple browsers, not just devices
- Individual v. household matching
- Used for interest-based advertising, ad delivery (e.g., frequency capping), content optimization, analytics, fraud prevention, and other purposes



How does it work?

- Deterministic v. Probabilistic
  - ***Deterministic***: User account logins or other identifiers (such as email address, often in random or obfuscated form) are used to link devices and provide high level of confidence that devices are shared by the same user
  - ***Probabilistic***: Device attributes are used to determine statistical likelihood that browsers or devices are shared by same user or household (e.g., device IDs, IP address, time/date, operating system, etc.)
- Matching information is often stored in device "graph"
- Audience segments from one device may be associated with other devices

DAA Guidance on Data Used Across Devices

Earlier this month, DAA released *Application of the DAA Principles of Transparency and Control to Data Used Across Devices*

- **Transparency**
  - Prior guidance applied to data collected and used on the specific computer (e.g., browser) or device from which data was collected
  - Under new guidance, must disclose "***the fact that data collected from a particular browser or device may be used with another computer or device that is linked to the browser or device on which such data was collected***."
  - Other principles apply, e.g., first- and third-party notice, enhanced notice, disclosure/consent for precise location used across devices, etc.
- **Control**
  - No multi-site or cross-app data from that device used on other devices
  - No multi-site or cross-app data from other devices used on that device
  - No transfer to a non-affiliate of any multi-site or cross-app data collected from the browser or device on which choice is exercised
  - Companies may use existing mechanisms (e.g., DAA opt-out webpage or AppChoices)
  - Choice does not apply to creation of "device graph" itself

Cross-Device Linking: Current Best Practices

Workshop held on November 16 (WilmerHale Alert available at https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179879882)

Best Practices for Notice and Transparency

- Provide notice and choice in a manner consistent with existing FTC and self-regulatory frameworks
- Disclose cross-device practices in privacy policy
  - What is collected and how are connections made among related devices;
  - How is cross-device information used for advertising or other purposes;
  - Is cross-device information combined with other data;
  - Is information shared with third parties and for what purposes;
  - How long is cross-device information retained; and
  - How can users opt out / limitations of opt-out.
- Provide "enhanced notice" through "Advertising Options" icon, or on webpages and apps where data is collected, that discloses cross-device practices and directs users to privacy policy and opt out
- Transparency tools to provide user visibility into cross-device connections

Cross-Device Linking: Current Best Practices

Choice

- At a minimum, choice should apply to the specific browser or device from which the user opts out (*see, e.g.*, DAA cross-device guidance)
- Opt-out scope and functionality may differ across industry as technology evolves
  - One device or all connected devices?
  - Interest-based advertising or all cross-device linking? If the latter, are there exceptions (e.g., fraud prevention or ad reporting)?
  - How to maintain a persistent opt-out? Apps/Browsers/Statistical IDs?
- Key is to ensure that opt-out descriptions are clear, conspicuous, and accurate, and that opt-out works as intended 100% of the time

2012 *BlueCava, Inc.* decision from BBB provides early, useful example:

- Privacy policy allegedly did not clearly explain that online activity could be tracked across devices and used for advertising purposes
- Description of opt-out allegedly was ambiguous as to whether opt-out would be honored on one device or across all devices

Lessons from the Telephone Consumer Protection Act (TCPA)

The Telephone Consumer Protection Act

- The **Telephone Consumer Protection Act ("TCPA")** regulates telemarketing and the use of automated telephone equipment for voice calls, faxes, and text messages.
- The TCPA provides for a private right of action and colossal statutory damages, making it a favorite of class-action plaintiffs: damages start at $500 and rise up to $1,500 ***per recipient*** for ***each text message*** sent.
- Consent is required for nearly all text messages. And for ***commercial*** text messages, "prior express ***written*** consent" is required.
  - There is *no exception* for a pre-existing business relationship.
  - Consent may be revoked.
  - Consent does not pass with a phone number that is reassigned.
- Certain types of non-commercial text messages may be permissible under limited TCPA exceptions, but reliance on exceptions can be risky.

Text Message Litigation Under the TCPA

Plaintiffs have challenged many different forms and categories of text messages under the TCPA:

- Commercial text messages without consumer consent.
  - Given widespread awareness of the TCPA, it is increasingly rare to see commercial text "blasts" to random telephone numbers, but plaintiffs frequently argue defects in consumer consent.
- Text messages that exceed the scope of consent provided.
- "Confirmatory" text messages acknowledging consumer opt-out.
- "Informational" text messages sent for the consumer's benefit.
- Internet-to-phone text message conversions.
- Smart phone applications with SMS technology.
- **The Takeaway** – Assume that **any** SMS-based communication with a consumer cell phone may be subject to TCPA scrutiny.

FCC 2015 TCPA Declaratory Ruling and Order

- Omnibus ruling resolved a backlog of nearly two dozen pending petitions for clarification.
- Billed as "strengthening consumer protections" against telemarketing calls/texts.
- The Order focuses on the following areas:
  - Confirming that text messages are "calls" under the TCPA
  - Definition of "automatic telephone dialing system" (ATDS) or "autodialer"
  - Establishing and revoking consent
  - Reassigned telephone numbers
  - Internet-to-phone messaging
  - Limited exceptions for certain "pro consumer" messages
  - Call-blocking technology

2015 FCC Order: Autodialer Definition

The Order resolved petitions seeking clarity on the definition of an "automatic telephone dialing system" or "autodialer."

- The TCPA defines an autodialer as equipment that has the **capacity** to "store or produce numbers . . . using a random or sequential number generator" and "to dial such numbers."
- Recurring disagreement as to whether "capacity" refers to current or potential capacity.
- **FCC Ruling** – "Potential capacity" controls:

- The Order states that "the capacity of an autodialer is not limited to its current configuration but also **includes potential functionalities**"

- The Order appears to acknowledge that most modern-day smartphones would fall within the FCC's broad interpretation

2015 FCC Order: Reassigned Numbers

The Order rejected petitions seeking broad exceptions for text messages sent to reassigned phone numbers.

- One of the most difficult issues that companies face with respect to the TCPA.
- The FCC has acknowledged that there is no comprehensive database or other guaranteed way for callers to identify reassigned mobile numbers.
- **FCC Ruling** – A "one-call" safe harbor:
  - Consent does not pass with a mobile phone number that is reassigned.
  - "One-call" exception: no TCPA liability for first call to reassigned number.
  - Any calls afterward are subject to TCPA liability, even if the caller does not receive actual notice of the reassigned number.
  - The ruling places the burden squarely on the caller to discover reassigned numbers and cease text messages.

2015 FCC Order: Revocation of Consent

The Order clarified how consumers can revoke their prior express consent.

- The TCPA itself is silent on whether consent, once provided, can be revoked.
- Courts were previously split on the significance of that silence, including whether consent could be revoked at all.
- **FCC Ruling** – Consumers may revoke consent through any "reasonable means."
  - Rejected petitions arguing that companies should be able to designate the specific way that a consumer must revoke consent.
  - "Reasonable means" would include, "among other possibilities": (1) consumer-initiated calls, (2) requests made in response to a call/text, and (3) oral requests at an in-store bill payment location.
  - Some argue that the standard provides unclear guidance to businesses.

2015 FCC Order: Other Rules for Text Messages

- **SMS Messages Are "Calls"** – The FCC reaffirmed its position that text messages are subject to the same consumer protections under the TCPA as voice calls.
- **Internet-to-Phone Text Messages** – The FCC clarified that such messages are the functional equivalent of SMS text messages and can require consent per the TCPA.
  - Internet-to-phone text messages originate as e-mails and are sent to an e-mail address in the form of the recipient's wireless telephone number and the carrier's domain name.
  - Significant clarification, because some had believed these messages were subject to only the CAN-SPAM Act, and not the TCPA.
- **One-Time "Call-to-Action" Texts** – The FCC clarified that one-time messages sent in response to consumer texts requesting information do not violate the TCPA.

2015 FCC Order: Dissenting Opinions

There were two dissents to the Declaratory Ruling and Order that were highly critical of certain aspects of the ruling.

- **On "Potential Capacity"** – The ruling "transforms the TCPA . . . into an unpredictable shotgun blast covering virtually all communications devices."
- **On Revocation of Consent** – "Congress did not address" this issue in the TCPA and "the FCC should not presume to act in its stead."
- **On Reassigned Numbers** – The one-time exception offers "fake relief" because it "expects callers to divine from mere silence the current status of a telephone number" and enables "consumers acting in bad faith to entrap legitimate companies."

2015 FCC Order: Appeals

- The Declaratory Ruling and Order is subject to appeal.
- As expected, several petitions for review were filed.
- The most controversial aspects of the Order have been challenged:
  - The acceptance of "potential capacity" over "present capacity" in defining an autodialer.
  - The limited exception for reassigned numbers.
  - The ability to revoke consent "by any reasonable means."
- The appeals have been consolidated and assigned to the D.C. Circuit.

Best Practices in an Expanded TCPA World

Do:

- Make consent disclosures clear, conspicuous, accurate, and detailed.
- Maintain complete and accurate records of consumer consent for at least four years after sending text messages.
- Have in place procedures to process opt-out requests in any manner, including via text, phone call, email, or web form.
- Require third-party vendors/partners to comply with the TCPA.

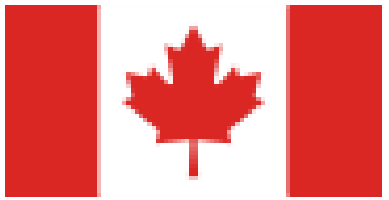
Do Not:

- Assume that you are not using an autodialer – it is the ***capacity*** to generate and call numbers that matters.
- Assume that consent remains "current" – be wary of consent obtained years ago, and take steps to identify recycled numbers.
- Place unnecessary restrictions on the scope of consent – get the consent you need to send the number and type of messages you may wish to send in the future.

Key Differences in Canada, the EU, and APEC

Key Differences: Canada

- **Canada's Anti-Spam Legislation ("CASL")**. Governs content and other features of emails, texts, and other "commercial electronic messages."
  - ***Includes mobile apps with text messaging or instant messaging features***
  - Express, ***opt-in consent*** generally is required to send commercial messages
  - Imposes content and other requirements for even ***transactional*** messages, including a link to the company's opt-out mechanism
  - Penalties of up to $10 million, as well as ***personal liability*** and criminal charges
- Messages must include postal address *and* phone, website, or email address
  - ***Information may be made available via clear and prominent link to a "readily accessible" web page***
- CASL provides exceptions to the opt-in consent requirement, including:
  - Messages sent in certain existing business relationships
  - Responses to an inquiry, request, or complaint
  - Initial messages sent subsequent to a referral
  - Some messages sent to disclosed or published addresses

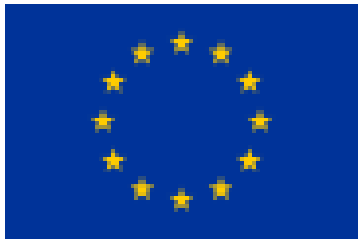


- CASL took effect in 2014 and regulators already have issued substantial fines

Key Differences: EU

- **Data Protection Directive (95/46/EC)**

  The scope of the EU's data protection requirements for ***personal data*** are broader than in the U.S.—potentially including mobile device IDs, IP addresses, and cookie IDs



- **Article 29 Working Party Opinion 02/2013 on Apps on Smart Devices**
  - *"The key data protection risks to end users are the lack of transparency and awareness of the types of processing an app may undertake combined with a lack of meaningful consent from end users before that processing takes place."*
  - Establishes that consent must be freely given, specific, and informed
    - Give users choice to cancel or stop installation, not just click "Yes I accept"
    - Provide users with necessary information prior to installation or prior to processing
    - Obtain individualized consents for processing different types of data
  - Encourages privacy by design and other data protection measures
    - Purpose limitation and data minimization
    - Clear and conspicuous notice (including "layered" notices, icons, or pop-ups)
    - Security, data retention, user access rights, and protection of children

Key Differences: EU

- **Article 5.1 of ePrivacy Directive (2002/58/EC) (as amended by Directive 2009/136/EC)**

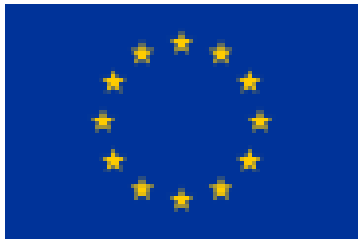
  Requires notice and consent for cookies and other tracking technologies

- **Article 29 Working Party Opinion on Device Fingerprinting (Nov. 25, 2014)**

  Clarified that the ePrivacy Directive applies to device fingerprinting, broadly defined to mean "a set of information that can be used to single out, link, or infer a user, user agent or device over time"

  - The Opinion noted that fingerprinting may occur on mobile apps and other Internet-connected devices
  - The reasoning could apply equally to similar technologies, such as mobile IDs

Key Differences: EU



- **Article 13 of ePrivacy Directive (2002/58/EC).**
  Imposes requirements with respect to ***texts and other electronic messages*** used for direct marketing.
  - Consent required for direct marketing messages
  - Business relationship exception where a customer provides electronic contact details "in the context of the sale of" a product or service, and the address is used to directly market the company's "own similar products or services"
  - Customers must "clearly and distinctly [be] given the opportunity to object, free of charge and in an easy manner, to" marketing messages when their address is collected and "on the occasion of each message"

- **Article 29 Working Party Opinion 2/2010 on Online Behavioral Advertising (June 22, 2010)**

  Addresses how the ePrivacy Directive applies to advertising technologies
  - Clarifies that placing cookies on a device for IBA requires prior opt-in consent
  - Reasoning applies equally to other practices, such as cross-app and cross-device targeting

Key Differences: APEC

- **Privacy laws and enforcement vary significantly across APEC region**
  - Eleven countries have comprehensive privacy laws (e.g., Australia, Hong Kong, India, Japan, Macau, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan)
  - Other countries have taken a piecemeal privacy approach (e.g., China)
  - Notice and choice are common elements, although some countries require individualized consent for processing certain information (e.g., South Korea)
- **Recent efforts have focused on mobile apps**
  - In March 2014, the Global Privacy Enforcement Network (GPEN) released the results of a privacy sweep of over 1,200 mobile apps and concluded that a large percentage of mobile apps do not provide adequate notice to consumers
    - In December 2014, privacy commissioners from Hong Kong, South Korea, New Zealand, Canada, and the UK issued an open letter to seven leading mobile app marketplaces asking them to make privacy policies available to users prior to download
  - South Korea issued guidance on mobile application privacy in August 2015 and stated that it would begin enforcement in October 2015
    - Requires consent for collection of personal information, such as location

"Must Haves"

- Ensure that the Privacy Policy covers mobile apps *and* appears within the app
- Provide just-in-time notice and obtain consent for location, contacts, and sensitive device data
- Use platform advertising IDs and follow Apple and Google terms
- Disclose cross-app and/or cross-device data collection and how you respond to "Limit Ad Tracking"
- Make sure that opt out is deterministic and works 100% of the time for *that device*
- Obtain opt-in consent for text messages
- Evaluate legal requirements in relevant jurisdictions before launching programs outside the U.S.
- Integrate privacy by design into data security program

"Should Haves"

- Make the Privacy Policy available through app stores prior to download
- Use icons and a privacy dashboard to give consumers information and choices about in-app data collection
- Participate in DAA Ad Choices program for interest-based advertising (including retargeting)
- Use "Limit Ad Tracking" signals to opt out devices from data *collection*
- Respect opt-out *across devices, to the extent possible,* and provide transparency tool to consumers
- Continue to pay close attention to laws, enforcement trends, and guidance from emerging regulators, self-regulatory bodies, and countries outside the U.S.

Any Questions?

Thank You and Contact Information

Reed Freeman
Partner; Co-Chair
Cybersecurity, Privacy and Communications Practice
WilmerHale

+1 202 663 6267
Reed.Freeman@wilmerhale.com
http://www.wilmerhale.com/Reed_Freeman/

Heather Zachary
Partner
WilmerHale

+1 202 663 6794
Heather.Zachary@wilmerhale.com
http://www.wilmerhale.com/Heather_Zachary/

**WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.*