Morgan Lewis

TECHNOLOGY MAY-RATHON

Text Messages, Robocalls, and Auto-Dialers: What's New in a Big Year for the Telephone Consumer Protection Act

May 10, 2021
Ezra Church
Ron Del Sesto
Julian Williams

Presenters

Ezra D. Church

Ronald W. Del Sesto, Jr.

Julian C. Williams

Morgan Lewis

Overview

- Background
- Express Written Consent
- Summary of Consent Requirements
- Litigation Defenses
- Key Issues for 2021
  - FCC Order implementing STIR/SHAKEN
  - COVID-19 FCC declaratory orders
  - Reassigned number database
  - *Barr v. American Association of Political Consultants Inc.*
  - *Facebook v. Duguid et al.*
  - Revocation of consent

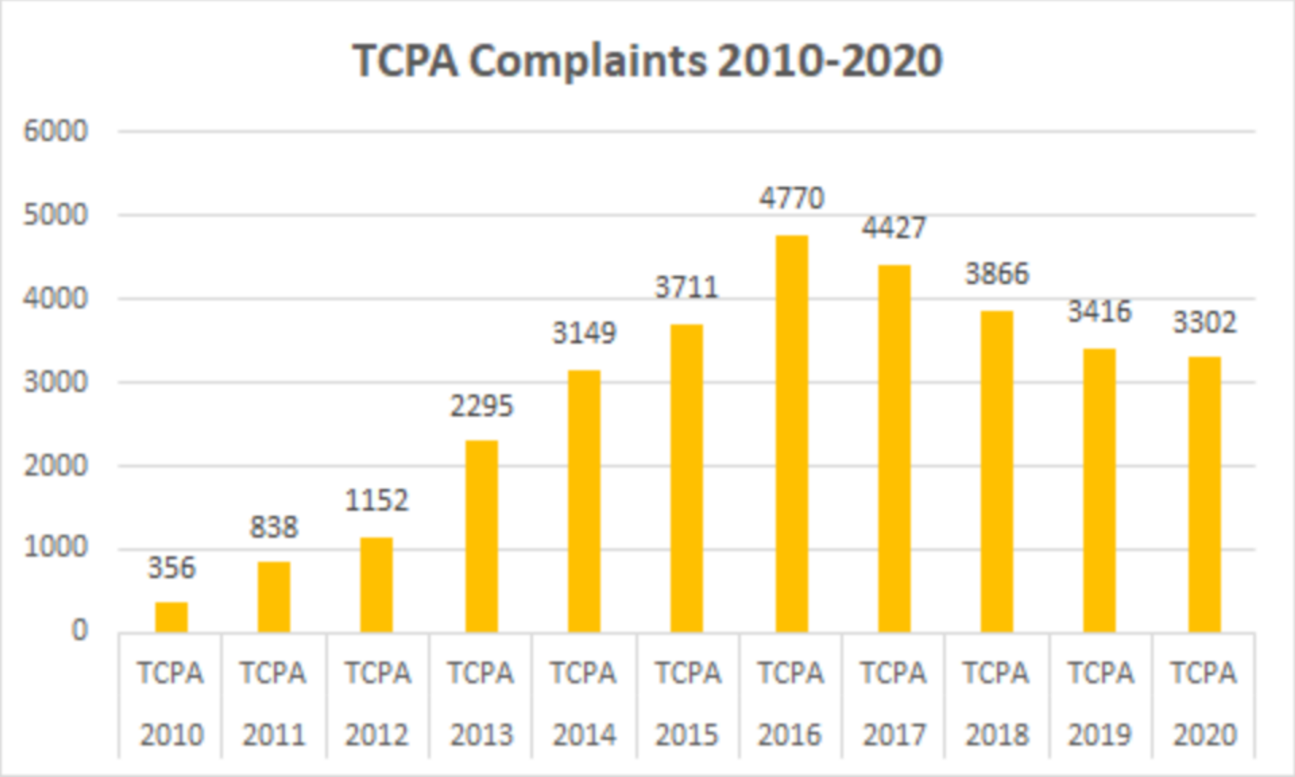
Background

- Telephone Consumer Protection Act of 1991, 47 U.S.C. section 227 (TCPA):
  - Prohibits (a) auto-dialed or prerecorded calls without consent (includes text messages) and (b) unsolicited ads sent to fax machines
  - Statutory damages of $500 per violation; treble damages for willful or knowing violations
  - Key defenses:
    - Express consent
    - Text not sent from auto-dialer

Background (cont.)

- Passed in 1991 to regulate robocalling and unsolicited faxes
- Expanded to include text messaging in 2003
- FCC has primary jurisdiction to interpret the TCPA
- FCC, FTC, and State AGs can enforce the act and it includes a private right of action
- $500 per violation; trebled if willful
- One of the most litigated consumer protection statutes

TCPA Complaints from 2010-2020



Express Written Consent

- To get consent, consumers must:
  - receive a clear and conspicuous disclosure of the consequences of providing consent; and
  - agree unambiguously to receive the calls at a designated number.
- Written consent must also include:
  - specific seller, including affiliates, that will be calling or sending messages;
  - that consent is not a condition of purchase, if applicable;
  - that the consumer can revoke at any time; and
  - that the consumer understands that the wireless carrier may impose charges.

Express Written Consent (cont.)

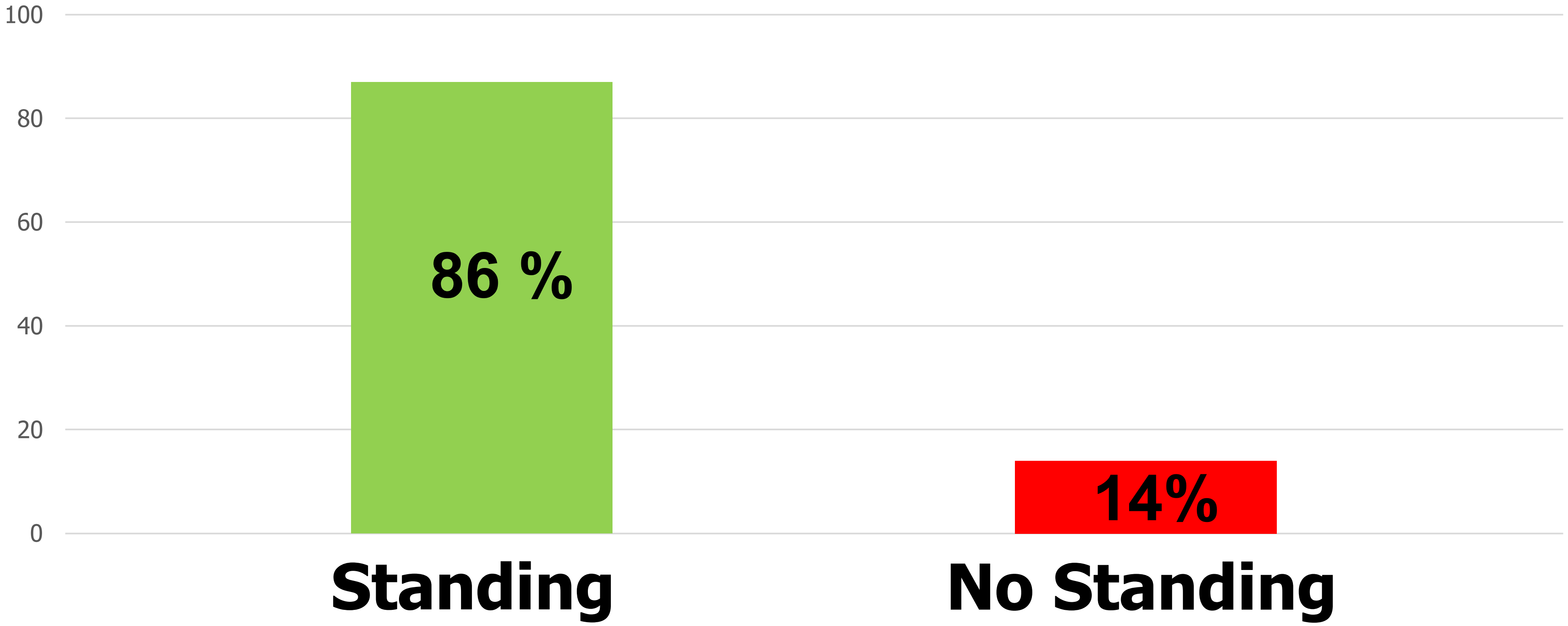
- Compliance with E-SIGN Act is sufficient; no prechecked box
- No “established business relationship” exemption (used to be available for prerecorded calls to landlines)
- “Purely informational calls” are exempt
  - “bank account balance, credit card fraud alert, package delivery, and school closing information”
- “Should any question about consent arise, the seller will bear the burden of demonstrating that a clear and conspicuous disclosure was provided and that unambiguous consent was obtained”

Consent as a Defense to Class Certification

Defendants have been successful in using consent to defeat class certification:

- *Selby v. LVNV*, No. 13-cv-01383, 2016 WL 6677928 (S.D. Cal. June 22, 2016): Individual inquiries into just how consent was obtained could not be avoided by simply excluding from the proposed class those individuals who had provided a cell phone number in the underlying transaction.
- *Stein v. Monterey Financial Services Inc.,* No. 2:13-cv-01336, 2017 WL 412874 (N.D. Ala. Jan. 31, 2017): Finding the difference between the defendant asking customers "What's a good home phone number for you?" and "Is this a valid contact number?" significant in determining that the defendant engaged in nonuniform behavior for collecting consent.
- *Ung v. Universal Acceptance Corp.*, No. 15-127, 2017 WL 354238 (D. Minn. Jan. 24, 2017): "Liability . . . will hinge on whether the class member orally consented to be called when contacted by Universal; voluntarily provided his or her cell phone number, either directly or through the car purchaser; appeared at the time of the purchase and agreed to be contacted; or provided his or her consent in some other way."
- *Blake Tishman, P.A. v. Baptist Health S. Fla., Inc.*, No. 17-62230-CIV, 2019 WL 3890506 (S.D. Fla. June 10, 2019): "The Court finds that the Plaintiff has failed to establish, as required by Rule 23(b)(3), that class-wide questions of law or fact predominate over questions requiring individualized inquiry as to each class member, because an individualized inquiry is required to determine whether each class member provided permission or consent."
- *Hirsch v. USHealth Advisors, LLC*, 337 F.R.D. 118 (N.D. Tex. 2020): Denying class certification because "[d]efendants' obtained phone numbers from numerous sources—preventing any attempt to show consent from a single source or "in one stroke."

Standing Post-Spokeo: TCPA



Morgan Lewis

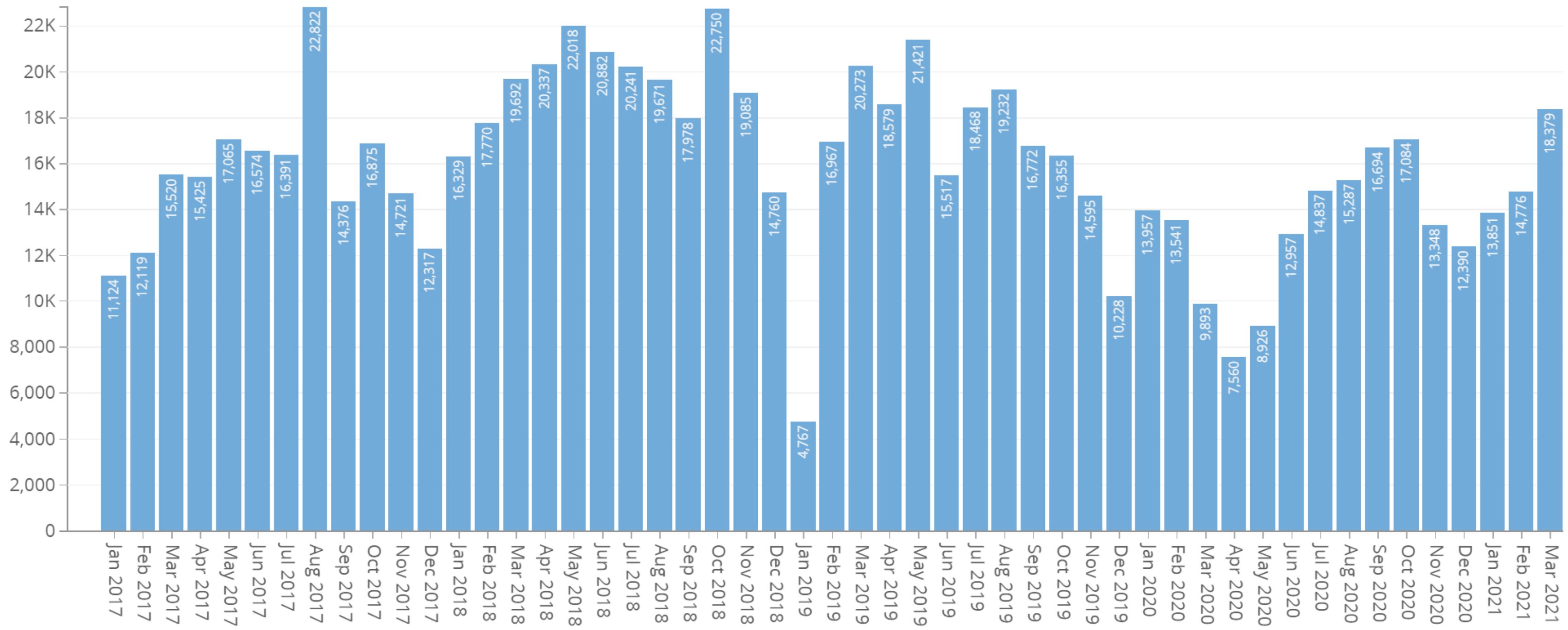
TCPA – Key Issues for 2021

- FCC Order implementing STIR/SHAKEN
- FCC Declaratory Orders concerning COVID-19
- TRACED Act revisions to the TCPA rules
- Reassigned number database
- Supreme Court's decision in *Barr v. American Association of Political Consultants Inc.* invalidating the government-debt exception to the TCPA as unconstitutional
- Supreme Court's recent decision in *Facebook v. Duguid et al.* clarifying the definition of an "automatic telephone dialing system" or ATDS
- Standards for revocation of consent are in flux
  - *Medley v. Dish Network, LLC*, 958 F.3d 1063, 1070 (11th Cir. 2020) (holding that "common law contract principles do not allow unilateral revocation of consent when given as consideration in a bargained-for agreement")

FCC – Combat Against Robocalling

- Multi-Pronged Approach
  - Attempting to clamp down on “spoofing”
  - Fantastic Fines for Violations of its Truth-in-Caller ID Rules
  - Extended Truth-in-Caller ID Rules to Foreign calls and text messages
  - Selected a consortium of industry participants to lead traceback efforts
  - Adopted new rules allowing for call blocking in certain circumstances

Unwanted Call Complaints Filed with the FCC from 2017-2021



Congress Jumps In

- Caller Identification – *RAY BAUM'S Act*
  - *Implementing Section 503 of the RAY BAUM'S Act; Rules and Regulation Implementing the Truth in Caller ID Act of 2009*
- Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (TRACED Act)
  - *Implementing Section 13(d) of the Pallone-Thune Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, Report and Order and FNPRM
  - *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*

STIR/SHAKEN

- Secure Telephony Identity Revisited (STIR); Signature-based Handling of Asserted information using toKENs (SHAKEN)
  - Establishes industry standards and protocols for exchanging traffic allowing for verifying call information and easing tracing calls as they traverse different carriers' networks
  - Two components: (1) process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call
  - Relies on digital "certificates" to ensure trust

STIR/SHAKEN (cont'd)

- Governance Model
  1. Governance Authority
  2. Policy Administrator
  3. Certification Authorities
  4. Voice Service Providers
- TRACED Act directed the FCC to require by June 30, 2021, all voice service providers to implement STIR/SHAKEN

FCC Order Implementing STIR/SHAKEN

- March 2020 – *First Caller ID Authentication Report and Order and Further Notice*
- October 2020 – Second Report and Order
- December 2020 – Fourth Report and Order
- December 2020 – TCPA Report and Order
- April 20, 2021 – Public Notice Establishing Mandatory Database for Voice Service Providers
- FCC rules require providers to implement STIR/SHAKEN in the Internet Protocol (IP) portions of their networks by June 30, 2021. In September 2020, the FCC further implemented Congressional direction from the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) and adopted more rules to ensure that even those providers unable to implement STIR/SHAKEN right away are still taking steps to protect their customers from illegal robocalls.
- As of April 20, 2021, the FCC requires that all providers certify that they have fully implemented STIR/SHAKEN or have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls. All providers are required to submit to the Robocall Mitigation Database the contact information for the personnel at their company responsible for robocall-mitigation related issues. Also, because the STIR/SHAKEN framework is only operational on IP networks, Commission rules also require providers using older forms of network technology to either upgrade their networks to IP or actively work to develop a caller ID authentication solution that is operational on non-IP networks.

FCC Declaratory Rulings Regarding COVID-19

- On March 20, 2020, the FCC issued a declaratory order “confirm[ing] that the COVID-19 pandemic constitutes an ‘emergency’ under the Telephone Consumer Protection Act (TCPA) and that consequently hospitals, health care providers, state and local health officials, and other government officials may lawfully communicate information about the novel coronavirus as well as mitigation measures without violating federal law.”
- On July 28, 2020, the FCC issued a clarification “confirm[ing] that calls and text messages made by or on behalf of commercial labs, health insurers, physicians, and pharmacies (health care entities) that, pursuant to guidance from federal, state, or local government officials, communicate with individuals who have tested positive for COVID-19 to provide them with information regarding donating their plasma after recovering, fall within the ‘emergency purposes’ exception to the Telephone Consumer Protection Act (TCPA).”

TRACED Act Revisions to the TCPA Rules

- Artificial or prerecorded voice messages “not made for a commercial purpose” can be placed to residential telephone lines.
- Limits such calls placed to three artificial or prerecorded voices calls within any consecutive 30-day period.
- Requires providing call recipients with and opt-out mechanism
- Applies to commercial calls not constituting telemarketing and tax-exempt nonprofit organization calls to a residence.
- HIPAA-related calls that deliver a healthcare message – one artificial or prerecorded voice call per day up to a maximum of three calls per week.

Reassigned Numbers Database

- FCC December 13, 2018 Order
  1. Establishes a nationwide database of reassigned numbers; all providers that obtain numbers directly or indirectly must report disconnection dates to central database
  2. Toll-Free Numbering Administrator must report disconnected numbers
  3. Establishes a 45-day minimum aging period for reassigning numbers (90-day maximum; toll-free numbers 4 months)
- Privacy Restrictions Associated with the Reassigned Number Database
  1. Database will contain recent date of permanent disconnections; no subscriber data.
  2. Response to queries limited to a “yes,” “no,” or “no data”
  3. Parties querying the database must certify to the limited purpose for which they are using the database

Reassigned Numbers Database (cont.)

- Safe Harbor:
  - Callers that make use of the database should not be subject to liability if the database reports that a number has not been reassigned and nevertheless it has been, and so a caller inadvertently calls a new consumer
  - Caller must have reasonably relied upon the database when making a particular call
  - Limited to the database established by the FCC Order
  - Callers must demonstrate that they appropriately checked the most recent update of the database and the database reported “No” when given either the date they contacted that consumer or the date on which the caller could be confident that the consumer could still be reached at that number
  - Callers bear the burden of proof and persuasion to show that they checked the database before making a call

Reassigned Numbers Database (cont.)

Implementation

- On February 8, 2021, the FCC released a Public Notice announcing the compliance date for the final rule related to the Reassigned Numbers Database.
- Beginning April 15, 2021, and every 15th day of each month thereafter, service providers must report permanent disconnections of their subscribers.
- Small service providers (100,000 or fewer domestic retail lines) have six additional months (until October 15, 2021) to begin reporting to the Reassigned Numbers Database Administrator.

Barr v. American Association of Political Consultants Inc.

- TCPA amended in 2015 to exempt calls relating to the collection of debts owed or guaranteed by the federal government.
- On July 6, 2020, the Supreme Court issued its decision in *Barr v. American Association of Political Consultants Inc.*, invalidating the government-debt exception to the TCPA as unconstitutional, but leaving the rest of the ban on autodialed calls intact.
- The Court concluded that through the government debt exception, Congress has impermissibly favored debt collection speech over political and other speech in violation of the First Amendment.
- District courts are split on the issue of whether *Barr* has any effect on the liability of calls other than Government collection calls.

Barr v. American Association of Political Consultants Inc. **(cont.)**

- Takeaways from *Barr*:
  - The TCPA remains the law of the land and is only strengthened by the decision.
  - In addition, the court appears to have been influenced in part by the perceived popularity of the TCPA, as Justice Kavanaugh notes that although Americans disagree about many things, they are "largely united in their disdain for robocalls.”
  - Also, the *Barr* decision may also be used to challenge other aspects of the TCPA, such as exceptions for package delivery and certain types of healthcare messages. Given the court's conclusion that the exception for government debt collection was unconstitutional because it "single[d] out specific subject matter for deferential treatment,” some may argue that the other exceptions are also problematic.

Revocation of Consent

- The TCPA does not elaborate on the processes by which consumers may validly revoke consent.
- The FCC's 2015 Order concluded that a "called party may revoke consent at any time and ***through any reasonable means***."
- In *ACA Int'l*, the DC Circuit upheld the FCC's 2015 ruling on revocation of consent, noting that establishing clearly-defined and simple opt-out methods is a way in which callers can protect themselves from liability: "callers will have every incentive to avoid TCPA liability by making available clearly-defined and easy-to-use opt-out methods. If recipients are afforded such options, any effort to sidestep the available methods in favor of idiosyncratic or imaginative revocation requests might well be seen as unreasonable."
  - In addition, the court stated that nothing in the FCC's 2015 order should be understood to speak to parties' ability to contractually agree upon revocation procedures.
- The DC Circuit offered two avenues that could be helpful to companies in avoiding TCPA litigation: (1) create clear and easy revocation methods and communicate those methods to consumers; and (2) negotiate the terms of revocation by contract.
- On May 1, 2020, the Eleventh Circuit held in a TCPA case that "common law contract principles do not allow unilateral revocation of consent when given as consideration in a bargained-for agreement." *See Medley v. Dish Network, LLC*, 958 F.3d 1063, 1070 (11th Cir. 2020).

Definition of “Autodialer”

- To be liable under the TCPA, call must be made with an “automatic telephone dialing system” or use a recorded message.
  - ATDS defined as “equipment which has the capacity (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.”
- The FCC’s 2015 Omnibus Order addressed the definition of an ATDS and broadened the statutory definition of **“capacity”** to encompass “potential functionalities” and “future possibility.”
- In *ACA Int’l. v. FCC*, 885 F.3d 687 (D.C. Cir. 2018), the DC Circuit held that the FCC’s interpretation of ATDS in its 2015 Order leaves affected parties “in a significant fog of uncertainty about how to determine if a device is an ATDS so as to bring into play the restrictions on unconsented calls.” The court did not provide any other guidance on the meaning of ATDS; instead, it found that any interpretation of “capacity” that includes smartphones is an unreasonable reading of the TCPA.

Post-*ACA Int'l*: Definition of "Autodialer"

- Post-*ACA Int'l*, Circuit Courts were split on the definition of an ATDS:
  - ***Marks v. Crunch San Diego, LLC*, 904 F.3d 1041 (9th Cir. 2018)** (holding that an ATDS is not limited to devices with the capacity to call numbers produced by a "random or sequential number generator" but also includes devices with the "capacity to dial stored numbers automatically)
  - ***Dominguez v. Yahoo, Inc.*, 894 F.3d 116, 119 (3d Cir. 2018)** ("[In light of the D.C. Circuit's holding, we interpret the statutory definition of an autodialer as we did prior to the issuance of [the] 2015 Declaratory Ruling … [t]he … question, then, is whether … the [device] ha[s] the present capacity to function as [an] autodialer.").
  - ***Herrick v. GoDaddy.com*, 312 F. Supp. 3d 792 (D. Ariz. 2019)** (holding that the *ACA Int'l* decision is binding on district courts in the Ninth Circuit and held that under prevailing Ninth Circuit law and *ACA Int'l*, the device at issue did not have the capacity to store or produce numbers to be dialed using a random or sequential number generator and that, even if it did, the fact that the system did not have the ability to dial without human intervention disqualified it from being an ATDS).

- The FCC issued a Public Notice on May 14, 2018
  1. What constitutes and ATDS? (a) capacity; (b) functions; (c) random or sequential number generator of an ATDS; and (d) making a call using an ATDS
  2. Reassigned numbers and meaning of "called party"
  3. Revocation of consent
  4. Certain rules relating to calls placed when collecting debts to federal government

Supreme Court’s Autodialer Decision

- *Facebook v. Duguid et al.* (April 1, 2021)—Long awaited clarification on the definition of an “automatic telephone dialing system,” key term under the Telephone Consumer Protection Act (TCPA).
- TCPA requires prior express consent for any call or text sent with an ATDS.
- Statutory definition says an ATDS is equipment with the capacity “to store or produce telephone numbers to be called, using a random or sequential number generator,” and to dial those numbers.
- Plaintiff argued that the phrase “using a random or sequential number generator” modified only “to produce”; Facebook said that it modified both “to produce” and “to store.”
- The Court addressed a question facing thousands of companies: Is a system that merely stores and calls/texts customer numbers automatically an ATDS?

Supreme Court's Autodialer Decision (cont.)

- Court Held: Ruled 9-0 for Facebook.
  - Applying simple rules of grammar, an ATDS must have the capacity either to store a telephone number using a random or sequential number generator OR to produce a number using a random or sequential number generator.
  - Context confirms this reading since Congress's concern was that ATDS technology would dial emergency lines randomly or tie up all the sequentially numbered lines at a single entity.
  - The Supreme Court cannot reinterpret the statute to encompass new technology.
- Reduces risk for companies who text and call customers. Systems that are just calling from a list are not an ATDS.
- But not correct that you do not need consent:
  - Do Not Call Rules still apply
  - "Capacity" question
  - State law
  - Congressional action?
- The *Facebook* decision narrows the interpretation of autodialer, as the capacity to store or produce numbers using a random or sequential number generation is required, and should curb at least some ATDS lawsuits. *See Montanez v. Future Vision Brain Bank, LLC*, No. 20-CV-02959-CMA-MEH, 2021 WL 1291182 (D. Colo. Apr. 7, 2021) ("The Supreme Court just provided clarity on this issue … h[olding] that an ATDS **'must have the capacity either to store a telephone number *using a random or sequential generator* or to produce a telephone number *using a random or sequential number generator.'*** As such, it is critical that a random or sequential number generator be utilized to constitute an ATDS. While the Supreme Court's decision elucidates the definition of an ATDS, that holding will prove far more relevant on a future motion for summary judgment than it does now."
- Application beyond TCPA

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "Stay Up to Date" button.

EZRA D. CHURCH

Ezra Church
Philadelphia
+1.215.963.5710
ezra.church@morganlewis.com

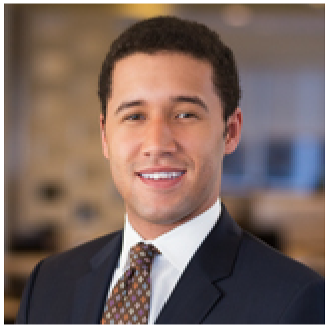
Ezra D. Church counsels and defends companies in privacy, cybersecurity, and other consumer protection matters. He helps clients manage data security and other crisis incidents and represents them in high-profile privacy and other class actions. Focused particularly on retail, ecommerce, and other consumer-facing firms, his practice is at the forefront of issues such as biometrics, artificial intelligence, location tracking, ad tech, and blockchain. Ezra is a Certified Information Privacy Professional (CIPP) and co-chair of the firm's Class Action Working Group. Ezra advises clients on compliance with data privacy and cybersecurity requirements such as the California Consumer Privacy Act (CCPA), the Gramm-Leach Bliley Act (GLBA), including Regulation S-P, Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) laws, the Telephone Consumer Protection Act (TCPA), the Fair Credit Reporting Act (FCRA), the Illinois Biometric Privacy Act (BIPA), the EU's General Data Protection Regulation (GDPR), and state data breach notification laws.

RONALD W. DEL SESTO, JR.

Ron Del Sesto
Washington, DC
+1.202.739.6023
ronald.delsesto@morganlewis.com

Ron Del Sesto represents technology companies on a broad range of issues including corporate, financial, regulatory, and cybersecurity. Ron also advises financial institutions, private equity firms and venture capital funds with respect to investments in the telecommunications, media, and technology (TMT) sectors. Ron also counsels clients on privacy issues that implicate a myriad of federal statutes and rules, including the FCC's Customer Proprietary Network Information (CPNI) rules; retention marketing and "winback" rules; the Telephone Consumer Protection Act (TCPA); the FTC's Identity Theft or Red Flag Rules; the Telemarketing Sales Rules; and the CAN SPAM Act. He advises clients with respect to the use of location-based data by mobile applications, assists clients in implementing "best practices" when handling personally identifiable information, and is familiar with the self-regulatory industry practices established by various trade associations as well as FTC rulings and other reports and analyses released by the FCC, the FTC, and state attorneys general that provide guidance to the industry.

JULIAN C. WILLIAMS



Julian Williams
Philadelphia
+1.215.963.5359
julian.williams@morganlewis.com

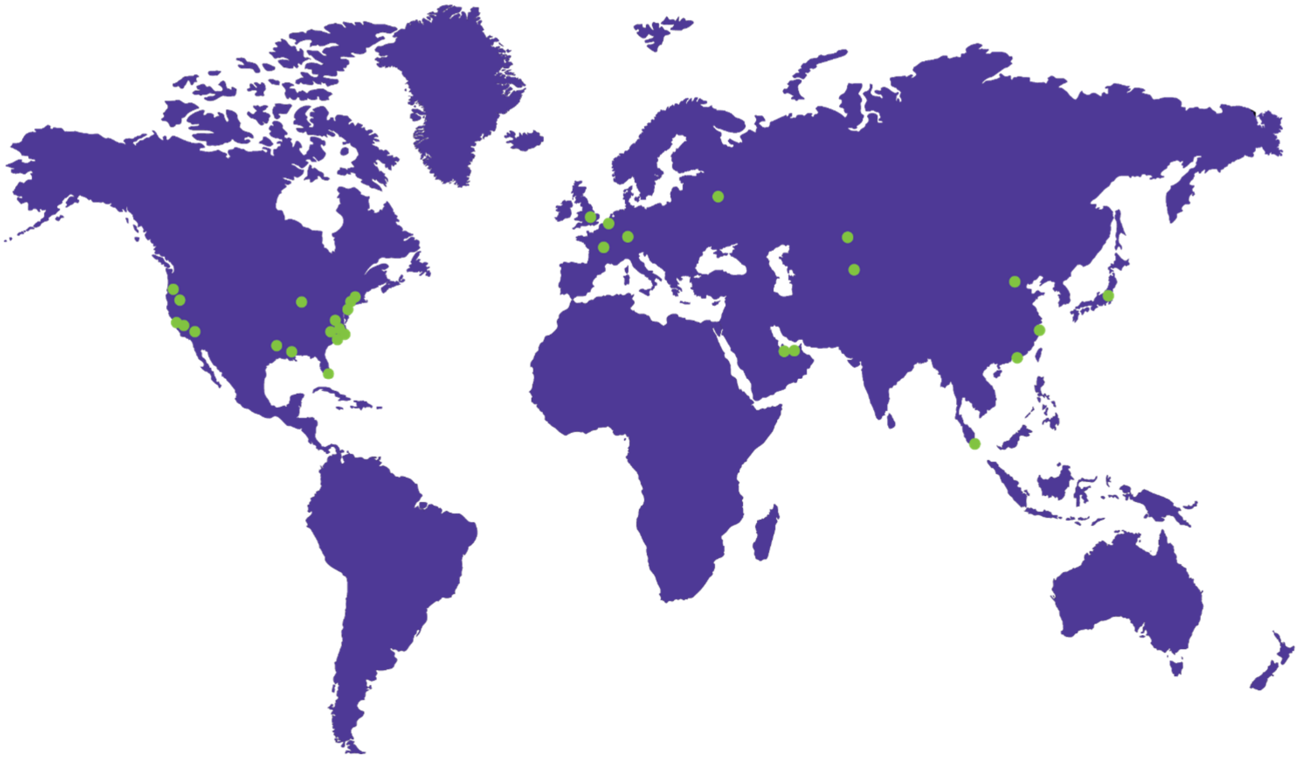
Julian C. Williams focuses his practice on class action lawsuits and complex commercial and product-related litigation. Julian understands the unique issues facing retail, ecommerce, and other consumer-facing companies. He also focuses on privacy and data security matters, and regularly counsels and represents clients in connection with these issues. Julian is a member of the firm’s retail and privacy and cybersecurity practices as well as its Class Action Working Group. His experience includes the requirements of the General Data Protection Regulation (GDPR), state data security laws, the Gramm-Leach Bliley Act (GLBA), and the Telephone Consumer Protection Act (TCPA).

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.