AN A.S. PRATT PUBLICATION
JUNE 2020
VOL. 6 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 NUMBER 5 JUNE 2020

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [131] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc.

For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

Anti-Robocall Bill Is Now Law

By Matthew S. DelNero, Yaron Dori, and Rafael Reyneri*

This article discusses the TRACED Act, which was enacted to decrease unwanted robocalls, and which directs the Federal Communications Commission to revise certain rules under the Telephone Consumer Protection Act to accomplish this objective.

The recently enacted TRACED Act,[1] which is aimed at curbing unwanted robocalls, also directs the Federal Communications Commission ("FCC") to revise certain rules under the Telephone Consumer Protection Act ("TCPA") to accomplish this objective. Those revisions, however, are not expected to change typical TCPA compliance practices.

The TRACED Act is expected to primarily affect the practices of telephone carriers and entities that transmit high volumes of robocalls. It could, however, have a broader effect on entities that transmit large volumes of calls, including live-voice calls. This is because the new law requires the adoption of the Signature-based Handling of Asserted Information Using toKENs ("SHAKEN") and the Secure Telephone Identity Revisited ("STIR") (together, "SHAKEN/STIR") call authentication framework that, depending on its implementation, can end up blocking calls from numbers that transmit high volumes of calls. The new law provides carriers with an incentive to block and label all such calls by providing them with a safe harbor from liability for such action.

The new law also directs the FCC to regularly monitor and update Congress on the progress that carriers have made in adopting call authentication frameworks, as well as call blocking and labeling measures. That, in turn, could result in the FCC applying increased pressure on carriers to take such actions. As a result, the TRACED Act could increase the risk that high-volumes of calls will be blocked or mislabeled as spam.

More specifically, the TRACED Act:

CALL AUTHENTICATION AND CALL BLOCKING

- Directs the FCC within 18 months of enactment to require telephone carriers to implement the SHAKEN/STIR call authentication framework, though it permits the FCC to exempt from this requirement any carrier that would suffer undue hardship as a result of its imposition—for example, because the carrier's network relies on time division multiplexing ("TDM") rather than IP technology. However, any carrier so exempt still must adopt a robocall mitigation program to prevent unlawful robocalls from originating on its network.

---

* The authors, attorneys with Covington & Burling LLP, may be contacted at mdelnero@cov.com, ydori@cov.com, and rreyneri@cov.com, respectively.

[1] https://www.congress.gov/116/bills/s151/BILLS-116s151enr.xml.

- Directs the FCC to prohibit telephone carriers from charging consumers or small businesses for providing SHAKEN/STIR or other call authentication frameworks.
- Directs the FCC to, within one year of enactment, establish a safe harbor for telephone carriers that unintentionally or inadvertently block or mislabel telephone calls, and to establish rules governing the blocking and labeling of calls, including to provide consumers and callers with a redress mechanism.
- Directs the FCC to streamline the process by which telephone carriers can share information with the FCC regarding TCPA violations and calls that are not authenticated under SHAKEN/STIR.
- Directs the FCC to establish a registration process for an industry consortium tasked with leading industry efforts to trace back (i.e., determine the source of) unlawful robocalls.

ADDITIONAL TCPA RULES FOR ROBOCALLS

- Revises the FCC's existing authority to exempt certain types of calls from the TCPA's consent requirements to ensure that any such exemption includes limits on:

  (1) Who may make such calls;

  (2) Who may receive such calls; and

  (3) The number of calls that an entity may place to a specific recipient.

- Directs the FCC to commence a proceeding to help subscribers avoid receiving unwanted robocalls from numbers that are not authenticated under SHAKEN/STIR, including the ability to block calls from unauthenticated numbers.
- Directs the FCC to determine whether its numbering policies could be modified to reduce access to telephone numbers for TCPA violators, and authorizes the FCC to promulgate regulations restricting access to numbers and imposing civil forfeitures for violations of such regulations.
- Directs the FCC to publish a report describing the progress it has made toward establishing the reassigned numbers database (a database that would allow callers to confirm whether a number they intend to dial has been reassigned to a different subscriber).

INCREASED ENFORCEMENT

- Expands the FCC's authority to impose civil forfeiture penalties for violations of the TCPA. Previously, the FCC was unable to impose penalties on non-licensee

first-time offenders; the TRACED Act removes that restriction and extends the applicable statute of limitations for FCC enforcement actions to four years. The law also grants the FCC authority to impose an additional civil forfeiture penalty for violations of the TCPA's automated dialing provisions, with penalties up to $10,000 per intentional violation.

- Establishes an interagency working group charged with evaluating methods of increasing TCPA enforcement, including criminal prosecutions.
- Directs the FCC's Enforcement Bureau to provide the U.S. Department of Justice with evidence of willful, knowing, and repeated robocall violations.
- Directs the FCC to commence a proceeding aimed at curbing "one-ring scams," defined to mean "a scam in which a [typically overseas] caller makes a call and allows the call to ring the called party for a short duration, in order to prompt the called party to return the call, thereby subjecting the called party to charges."
- Directs the FCC to establish the "Hospital Robocall Working Group," aimed at reducing unlawful robocalls to hospitals.