AN A.S. PRATT PUBLICATION
SEPTEMBER 2025
VOL. 11 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 7** **September 2025**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Sidley Austin LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2025 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires 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, 631.291.5541. 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Steering Clear of ECPA Liability: What Connected Vehicle Companies Should Know About Responding to Government Process

By Ian L. Barlow, Brandon J. Moss and Elizabeth K. Drill*

In this article, the authors explain that connected vehicle companies must be intentional about routinely assessing new features for potential Electronic Communications Privacy Act implications to be prepared to act quickly when served with government process.

"Connected vehicles," or vehicles that can connect to external systems, provide a variety of benefits to customers, including smart routing, voice-enabled assistance, improved driver safety, and in-vehicle entertainment. But in many cases, taking advantage of such innovative features requires drivers to share location, driving habits, personal communications, and even biometric data with companies that have not historically stored such customer data and communications – car manufacturers.

That trove of sensitive data brings unique legal obligations, wrinkles and, ultimately, risks. For instance, connected vehicle companies may increasingly find themselves critical players in law enforcement investigations and civil discovery, a role that will likely bring them face to face with the Electronic Communications Privacy Act (ECPA). Initially passed in 1986, ECPA governs the circumstances under which companies that provide communications services or store communications may disclose customer data and communications (most notably, to the U.S. government). Despite predating the modern internet, ECPA is quickly becoming a critical consideration for the companies behind the "smart" products customers increasingly demand – including, in some circumstances, connected cars. To avoid liability and reputational harm, in-house counsel for connected vehicle companies must be alert to ECPA's restrictions on disclosure and safe harbors.

ECPA OVERVIEW

ECPA consists of three main provisions: the Wiretap Act, the Stored Communications Act (SCA), and the Pen Register/Trap and Trace Act. Relevant here, the SCA regulates the disclosure of stored electronic communications and communications-related data by certain types of entities – namely, providers of electronic communication services (ECSs) and remote computing services (RCSs). The SCA prohibits those providers from disclosing electronic communications and related records and customer information to

* The authors, attorneys with Wiley Rein LLP, may be contacted at ibarlow@wiley.law, bmoss@wiley.law and edrill@wiley.law, respectively.

a third party, with limited exceptions.[1] For instance, it does not apply where, in the case of an ECS, the originator or an addressee or intended recipient of the communication consents to disclosure or where, in the case of an RCS, the subscriber consents to the disclosure.[2]

In addition to establishing prohibitions on sharing content and data, the SCA limits how the government can compel electronic records from covered providers through warrants, subpoenas, and court orders.

Specifically, it affords the content of communications held by ECS providers for 180 days or less the greatest degree of protection, requiring that government agencies obtain a warrant for such information.[3]

By contrast, to compel the content of electronic communications held by an ECS provider for longer than 180 days or the content of any electronic communications held by an RCS provider, the government must either (1) provide prior notice to the subscriber or customer and obtain a subpoena or court order, or (2) obtain a warrant.[4]

On the other end of the spectrum, the government only needs to issue certain specific subpoenas to compel certain basic subscriber records from ECS and RCS providers.[5] A third genre of process, a 2703(d) order, may compel other categories of non-content customer data.[6] However, as is often the case when applying old law to new technologies, where customer data fits into this rubric may not always be obvious.

COULD ECPA APPLY TO CONNECTED VEHICLE COMPANIES?

As discussed above, ECPA only applies to ECSs and RCSs. An ECS is defined under the ECPA as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[7]

Meanwhile, an RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[8] While both definitions are increasingly showing their age, modern courts continue to find ways to apply them to 21st century technologies. In addition to traditional telecommunications providers, ECSs may now include the following types of entities: internet service

[1] 18 U.S.C. § 2702(a)-(c).
[2] Id. § 2702(b)(3).
[3] Id. § 2703(a).
[4] Id. § 2703(a)-(b).
[5] Id. § 2703(c)(2).
[6] Id. § 2703(d).
[7] Id. § 2510(15).
[8] Id. § 2711(2).

providers, email service providers, messaging service providers, and applications that facilitate user communications.[9] And RCSs, oft referred to as "virtual filing cabinet[s],"[10] have been found to include internet service providers that store emails for users[11] and video sharing websites that store videos for users.[12]

Notably, whether an entity constitutes an ECS or an RCS is context and service-specific – application turns in large part on the information at issue.[13] Thus, depending on how a particular connected vehicle company's networks and systems operate, certain features could potentially implicate ECPA. For example, it is possible that a connected vehicle company that provides customers with automatic service notifications, connects drivers with third-party repair facilities, and then wirelessly transmits vehicle data to a repair shop on a driver's behalf could be acting as an ECS for purposes of those communications and related records. Providing the communications network and connectivity for these cars to communicate with other vehicles, traffic lights, and other roadside infrastructure (to enhance safety and traffic flow), may also be an ECS service. Another example is automatically contacting first responder services after an accident or emergency.

The same company might also be an RCS in several scenarios, such as when it:

- Compiles driver behavior data to allow motorists to monitor their own or their children's driving habits;
- Stores and maintains geolocation data so owners can track where their vehicle is being driven or has been driven by family members via an app, either in real time or after the fact;
- Offers personalized infotainment services that rely on the remote retrieval of cloud-based customer media preferences, voice profiles, or playlists;
- Stores and applies customer preferences for electric vehicle charging settings; or
- Wirelessly updates vehicle operating systems.

---

[9] See, e.g., Garcia v. City of Laredo, Tex., 702 F.3d 788, 792 (5th Cir. 2012) (observing that the SCA has been applied to communication service providers such as telephone companies, internet providers, and email service providers).

[10] See, e.g., Casillas v. Cypress Ins. Co., 770 F. App'x 329, 331 (9th Cir. 2019); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1022 (N.D. Cal. 2012).

[11] United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009).

[12] Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

[13] Low, 900 F. Supp. 2d at 1023.

BEST PRACTICES FOR RESPONDING TO GOVERNMENT PROCESS

Responding to government process for customer information should not be taken lightly. Under ECPA, covered entities can be civilly liable for improperly disclosing customer communications and records to the government.

Specifically, a person "aggrieved by any violation" of the SCA engaged in with a "knowing or intentional state of mind[,]" may recover equitable or declaratory relief, damages not less than $1,000, and punitive damages and attorney fees.[14] The SCA does include a "good faith" defense for companies that wrongfully disclose information on the reasonable, but mistaken, belief that a warrant, court order or subpoena required the disclosure.[15] However, providers are not entitled to assert that defense if they fail to reasonably assess the validity of legal process, overlook obvious deficiencies, or otherwise produce in response to process they know is invalid.

When receiving government process, connected vehicle companies should carefully consider whether they might be an ECS or RCS with respect to the information sought, and then evaluate the government request and their obligations. If the validity of the legal process for the information sought is questionable, counsel may consider taking the following steps to reduce the risk of unlawful production and potential liability:

- *Establish an Open Line of Communication With the Government.* Initiate a dialogue with the requesting law enforcement or administrative agency and inform the appropriate authorities of any concerns regarding complying with the subpoena. If the government cannot provide reasonable assurance, request additional process.

- *Narrow the Subpoena.* Attempt to narrow the subpoena to non-content, basic subscriber information (e.g., subscriber names, addresses, and phone numbers) to mitigate potential liability stemming from the production of stored customer records or content.

[14] 18 U.S.C. § 2707. On the other side of the coin, refusal to comply with a lawful court order or warrant could result in contempt proceedings, obstruction charges, or other sanctions.

[15] 18 U.S.C. § 2703(e) provides that "no cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter." 18 U.S.C. § 2707(e) provides that "a good faith reliance on – (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title); (2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of; is a complete defense to any civil or criminal action brought under this chapter or any other law."

- *Seek User Consent*. Seek user consent before disclosing certain sensitive data to the government, if feasible.

Furthermore, in-house counsel for connected vehicle companies should take proactive measures to ensure that their subpoena response programs comport with ECPA's requirements for customer data disclosure. And where no subpoena response program has been implemented yet, it would be prudent for in-house counsel to establish one to be better equipped to respond to the government's disclosure requests.

LOOKING AHEAD

With technology in cars rapidly evolving, the number of connected vehicle services resembling those associated with traditional ECS and RCS providers will continue to grow. Accordingly, connected vehicle companies must be intentional about routinely assessing new features for potential ECPA implications to be prepared to act quickly when served with process. They should also be on the lookout for case law expanding ECPA's reach to analogous industries.