AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2017
VOL. 3 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 2 | February/March 2017

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) 487-3000
Fax Number .... (518) 487-3584
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 ..... (518) 487-3000

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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [297] (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

(2017–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. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. 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, 718.224.2258. 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, 630 Central Ave., New Providence, NJ 07974.

Data Security and Breach Notification Requirements of FCC Privacy Order May Present Immediate Implementation Challenges for Many ISPs

By K.C. Halm and Adam Shoemaker*

In this article, the authors explain the new Federal Communications Commission's recent Privacy Order and the steps internet service providers should take to begin implementing the data security and breach notification requirements of the new order.

As internet service providers ("ISPs") continue to absorb the scope of the Federal Communications Commission's ("FCC") recent Privacy Order (the "Order"), one immediate question presents itself: what steps must ISPs take to begin implementing the data security and breach notification requirements of the new order? The fate of these regulations under the new Administration is unclear. However, they may survive in one form or another, and the core concepts underlying the FCC's order are likely to form the basis for best practices that regulators (whether the FCC or another agency) will expect ISPs to adopt even if the specific approach of the FCC's order is abandoned.

The Order mandates the adoption of new data security practices intended to ensure that ISP customers' proprietary information ("PI") is secure. Although the Order promotes what the Commission believes to be a "flexible" and "reasonable" approach to data security, ISPs are likely to disagree. Compliance with the new rules will require significant effort on the part of ISPs to design and implement a data security program that will withstand FCC scrutiny and that can hold up in an environment of increasing security risks. Likewise, the breach notification rules will require ISPs to implement a system that will allow them to react quickly and efficiently to notify customers, the FCC, and law enforcement organizations by providing pertinent information following an initial assessment of the breach and the potential harm. The Order, while voluminous, still lacks clarity in places, and the rules (if they remain in effect under the new Administration) may be supplemented by additional guidance leading up to, and after, their effective date. For now, ISPs should begin the process of designing and implementing a compliant data security program.

* K.C. Halm is a partner at Davis Wright Tremaine LLP counseling telecom, VoIP, and broadband internet service providers on a range of broadband policy and competition matters, including interconnection, number portability, intercarrier compensation, licensing, and tariff obligations. Adam Shoemaker is an associate at the firm focusing his practice on the regulatory needs of telecommunications and cable clients. The authors may be reached at kchalm@dwt.com and adamshoemaker@dwt.com, respectively.

DATA SECURITY

The new data security rules require ISPs to "take reasonable measures to protect customer [proprietary information] from unauthorized use, disclosure, or access." The definition of customer PI covers a wide range of data including precise geo-location, health, financial, and children's information, and Social Security numbers, and more. All of these disparate pieces of information must be protected by an ISP's data security program.

Rather than providing a list of specific practices that an ISP must implement to comply with the data security requirement, the FCC has chosen a flexible standard under which an ISP may design its own data security program tailored to its own operations, available tools, and industry best practices. In doing so, however, the ISP must consider four factors:

1) the nature and scope of the ISP's activities;
2) the sensitivity of the data it collects;
3) the size of the ISP; and
4) technical feasibility.

According to the Order, the FCC will consider the "reasonableness" of an ISP's data security program in light of these factors. For example, a small ISP that does not collect a large amount of customer PI would be permitted to implement a data security program with narrower scope and fewer dedicated resources, while an ISP that collects and uses large amounts of customer PI would be expected to devote considerable resources to securing that data. The technical feasibility factor is intended to prod ISPs to continually update their data security practices with the current technology so as to reduce the risk of harm as threats proliferate and threat profiles change.

GUIDANCE ON REASONABLE DATA SECURITY PRACTICES

While declining to mandate minimum data security standards, the Order does list a number of industry best practices and resources that it recommends ISPs consult in designing their data security programs. In particular, the FCC points to the National Institute of Standards and Technology's Cybersecurity Framework ("NIST CSF"), writing that "proper implementation of the NIST CSF, as part of a provider's overall risk management, would contribute significantly to reasonable data security." It also recommends that ISPs consult Federal Trade Commission ("FTC") guidance as well as materials related to the data security requirements under Health Insurance Portability and Accountability Act, the Gramm–Leach–Bliley Act, and other laws. The challenge in implementing the NIST CSF or any of these other sources of guidance is that each was created for a different context (e.g. the NIST CSF is intended to address data security for a wide range of government agencies) and the choice of which elements to adopt will be challenging. The Order's references to FTC guidance

suggest that FTC privacy cases may also provide helpful examples of security measures that are likely to be looked upon with approval by the FCC.

The Order also includes a number of recommended, but not required, data security practices. First, it recommends designating a "senior management official" to have personal responsibility for the implementation and ongoing monitoring of the data security program. Second, it advises ongoing training of employees and contractors about proper handling of customer PI. Third, it recommends that ISPs employ "robust" customer authentication practices to prevent unauthorized access. Fourth, the Order endorses using data minimization practices, including those included in the FTC's "Disposal Rule" to reduce risk by safely eliminating all non-essential customer PI.

Finally, the Order concludes that these same data security rules should extend to voice services as well, replacing the prior data security requirements in Part 64 of rules. Although the FCC claims that the flexible nature of the its data security requirement will make it less onerous on ISPs, particularly small providers who may not collect a large amount of customer PI, designing a compliant program without firm guidance creates its own daunting challenges.

Recent FCC precedent also provides additional guidance. A 2015 consent decree[1] with a telecommunications carrier marked the FCC's first attempt to expand the ambit of its regulation of data security practices following adoption of the Open Internet Order. The consent decree requires the carrier to develop and implement a data security program tailored to their size and the sensitivity of the data they collect. In addition, the consent decree also imposes an ongoing obligation to adjust and update the information security program upon material changes to the business operations, technology, arrangements with third parties, or internal or external threats to customer PI. Further, it requires the carrier to engage an independent monitor to review and audit the information security program upon its implementation.

Similarly, another 2015 consent decree[2] with a cable operator mandates a data security compliance program that may shed light on the types of provisions the FCC will look for in ISPs' data security programs. This consent decree requires the company to implement a thorough data minimization program that tracks the nature and extent of the customer proprietary network information ("CPNI") and PI collected and maintained by the company and third-party vendors, minimizes the number of employees who have access to this data based on a need-to-know basis, and restricts the company to collecting the "the minimum amount of PI necessary to provision and provide services." The consent decree also calls for annual audits of call center systems as well as annual penetration testing of selected systems and processes related to payment cards and collection and storage of PI/CPNI. Further, it requires

[1] https://apps.fcc.gov/edocs_public/attachmatch/DA-15-776A1.pdf.
[2] https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1241A1.pdf.

the cable operator to limit off-network access to PI and CPNI through an approved site-to-site virtual private network and mandates that the company implement a two-factor authentication system that has been reviewed by a third-party consulting firm.

BREACH NOTIFICATION

The new rule on breach notification[3] provides a comprehensive scheme that ISPs must use to notify customers, the FCC, and the Federal Bureau of Investigation ("FBI") of a data breach that implicates sensitive customer information. The FCC has defined a "breach" as any instance in which a person gains access to, uses, or discloses customer PI without, or exceeding, authorization. The rules provide that an ISP only needs to notify customers, the FCC and law enforcement officials if it concludes that the breach is likely to result in harm. However, because there is a presumption of harm, and because the Order defines "harm" so broadly, it remains to be seen how likely it is that ISPs will be able to rely on this exemption.

HARM-BASED EXEMPTION

A critical part of this rule is the exemption from the requirement to notify when the ISP "can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach." The Order provides some guidance on how an ISP is supposed to make this determination. First, the Order broadly defines "harm" to include not only financial, economic and identity theft – as most state breach notification statutes do – but also "physical and emotional harm," "reputational damage, personal embarrassment, or loss of control over the exposure of intimate personal details."

Second, the default presumption is that the breach will cause harm and the ISP must notify customers, the FCC, and law enforcement. This is true even if the data is encrypted. Only if, after investigation, the ISP can "reasonably" conclude that there is no harm may it forego notification.

Third, the Order establishes a "rebuttable presumption" that any breach involving sensitive PI poses a likelihood of harm. Notably, encryption of the information does not constitute a safe harbor under the FCC's rules. However, encryption is still prudent, because if information is encrypted, it is much less likely to pose harm when compromised. Finally, the intent of the party who created the breach (e.g. malicious hacking vs. inadvertent unauthorized access by an employee) is irrelevant; the likelihood of harm is the sole trigger for notification.

[3] 47 C.F.R. § 64.2006.

CONTENTS OF NOTIFICATION

The notification requirements themselves can be summarized fairly easily: upon discovery of a data breach, an ISP must notify affected customers within 30 calendar days by means of one of the following methods: email; letter; or other electronic means if agreed to by the customer. The notification must include:

- The date or estimated date range of the breach;
- A description of the customer PI believed to have been breached;
- Who to contact to learn more about the breach; and
- Contact information for the FCC.

If the compromised customer PI includes financial information, the notification must also include:

- Contact information for national credit reporting agencies; and
- Information about protection from identity theft

If a breach affects 5,000 or more customers, the ISP must also notify the FCC within seven business days of discovery, and at least three business days before notification is sent to affected customers. Upon discovering such a breach, the ISP must also notify the FBI and U.S. Secret Service within seven business days. If the breach affects fewer than 5,000 customers, the ISP must notify the FCC within 30 calendar days, but need not notify the FBI and Secret Service. In each case, the notification should be made through an FCC reporting system.

RECORDKEEPING REQUIREMENTS

The new rules require an ISP to maintain a record of every data breach within a two-year period except for those breaches that the ISP has reasonably determined resulted in no customer harm. The record must include all relevant dates and a copy of the customer notification.