AN A.S. PRATT PUBLICATION
AUGUST/SEPTEMBER 2015
VOL. 1 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 **NUMBER 1** **AUGUST/SEPTEMBER 2015**

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);
David Kalat, *Day One: The Origin Story of Computer Forensics*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (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

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

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.

FCC Becomes Latest Agency to Increase Consumer Privacy and Data Security Enforcement

By Paul C. Besozzi, Monica S. Desai, and Koyulyn K. Miller*

The Federal Communications Commission's Enforcement Bureau recently issued an Enforcement Advisory, providing initial guidance regarding the protection of personal and proprietary information by retail broadband internet access providers. The authors of this article discuss the Advisory and the trend toward aggressively protecting the sensitive personal information of consumers.

As attention and related widespread concerns about data security and exposure of sensitive private consumer information grows around the U.S., the Federal Communications Commission ("FCC") has joined the array of federal agencies using their enforcement tools to address these issues. While the Communications Act ("Act") for many years has afforded confidentiality protections for the details of a consumer's phone bill, over the last year, the FCC – led in particular by its Enforcement Bureau – has demonstrated an increased willingness to more broadly and aggressively protect "the sensitive personal information of American consumers from misappropriation, breach, and unlawful disclosure." This trend continued when the Bureau issued an Enforcement Advisory on May 20, 2015, providing initial guidance regarding the protection of personal and proprietary information by retail broadband internet access providers ("ISPs").

TRADITIONAL PRIVACY FOCUS

To be sure, under Section 222 of the Act, the FCC had always protected certain limited forms of customer information from misuse by those who collected it – primarily call detail information on individual phone bills (customer proprietary network information or "CPNI"). In 2013, the agency made clear that these protections applied equally to mobile carriers who collect such information. And most recently, last September, the agency settled a matter with Verizon for $7.4 million involving the company's failure to notify its customers about Verizon using their CPNI for marketing. A series of more recent enforcement actions, however, reflect that the agency has expanded its focus well beyond traditional concerns about protecting CPNI.

* Paul C. Besozzi and Monica S. Desai are partners, and Koyulyn K. Miller is an associate at Squire Patton Boggs. The authors may be contacted at paul.besozzi@squirepb.com, monica.desai@squirepb.com, and koyulyn.miller@squirepb.com, respectively.

FLEXING ENFORCEMENT AUTHORITY

The opening salvo in this expanded campaign occurred last October when the FCC proposed fines of $10 million on two telecommunications carriers that left unprotected, on publicly accessible websites, "proprietary information" they had gathered, including Social Security numbers. The FCC, in a 3-2 decision, concluded that Sections 222 and 201 of the Act impose a duty on carriers to protect such information, even though it was not the CPNI that the FCC had traditionally focused on in the past.

Then, in April of this year, the FCC entered into a $25 million settlement with AT&T to address data breaches by company employees at call centers in Mexico, Columbia, and the Philippines. Again, the enforcement action went beyond a focus on just CPNI to include the exposure of Social Security numbers and other identifying information.

To some degree these actions are not surprising. The Enforcement Bureau's senior leadership has substantial experience in data security and privacy protection, having worked in state attorneys general and other enforcement offices.

AND NOW THE INTERNET: ENFORCEMENT ADVISORY

Without question the major expansion of the commitment to privacy protection is the application of Section 222 to ISPs as newly classified telecommunications carriers. While the FCC recognized that its existing rules focused on voice type services and CPNI protections were a mismatch, the agency announced a commitment to developing a privacy regime under Section 222 for ISPs. It started that process with a workshop in April, which did not tip the agency's hand as to how it would proceed with enforcement. But on May 20 the Bureau issued an Enforcement Advisory warning ISPs that, after the effective date of the Open Internet Order on June 12, 2015, the Bureau will focus on "whether broadband providers are taking reasonable, good-faith steps to comply with Section 222." The Advisory also noted that the Bureau expects such providers to "employ effective privacy protections in line with their privacy policies and core tenets of basic privacy protections."

There are several points worth noting. First, the Advisory explains that the Bureau is available to provide informal and formal guidance on "how best to comply with Section 222," and states that although requesting guidance in the form of an advisory opinion is not required, the existence of such a request will tend to show good faith. Second, the Bureau repeated that it will only advise on "anticipated" conduct, consistent with direction in the Open Internet Order that hypothetical situations or past/ongoing conduct will not be the subject of advisory opinions. Third, the Commission – and the Bureau acting on delegated authority – reserved the right to change course from previously issued advisory opinions. Finally, the FCC warned in the Order

that it monitors press reports and other public information, which could lead to the initiation of an investigation.

JOINING FORCES

The FCC's focus on privacy protection is also reflected in its joining and publicizing its membership in international privacy groups. In April, the FCC joined the Asia Pacific Privacy Authorities, the principal international forum of privacy enforcement authorities in the Asia Pacific Region. This collaboration follows the FCC announcing its membership in the Global Privacy Enforcement Network, an international group of privacy enforcement regulators comprising approximately 50 data protection authorities. Significantly, in both of these memberships, it is the Enforcement Bureau that represents the FCC.

GOING FORWARD

It is clear that the FCC has staked out a role for itself both domestically and internationally in the protection of sensitive personal information by an expanded group of companies that gather such information. The scope of the requirements – particularly as they relate to the Internet – remain evolutionary and jurisdictional issues will need to be sorted out. But there is no question that the FCC is committed in a significant way to being involved in issues surrounding the security of sensitive information.