

AN A.S. PRATT PUBLICATION

JANUARY 2016

VOL. 2 • NO. 1

PRATT'S

PRIVACY & CYBERSECURITY LAW REPORT



LexisNexis®

EDITOR'S NOTE: INSURANCE

Steven A. Meyerowitz

DANGER IN THE WIRES: INSURANCE COVERAGE FOR CYBER RISKS

John L. Watkins

FTC HELD TO HAVE AUTHORITY TO REGULATE CYBERSECURITY PRACTICES UNDER SECTION 5 OF THE FTC ACT

Robert A. Swinger and Neal J. McLaughlin

WHEN BACKUP TAPES BECOME DISCOVERABLE - A COSTLY LESSON IN THE IMPORTANCE OF INFORMATION GOVERNANCE

Corey Lee and Meghan A. Podolny

COURT OF JUSTICE OF THE EUROPEAN UNION DECLARES EU COMMISSION'S U.S. SAFE HARBOR DECISION INVALID

Romano F. Subiotto and Christopher J. Cook

IN THE COURTS

Steven A. Meyerowitz

LEGISLATIVE AND REGULATORY DEVELOPMENTS

Steven A. Meyerowitz

INDUSTRY NEWS

Victoria Prussen Spears

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2

NUMBER 1

JANUARY 2016

Editor's Note: Insurance

Steven A. Meyerowitz

1

Danger in the Wires: Insurance Coverage for Cyber Risks

John L. Watkins

3

FTC Held to Have Authority to Regulate Cybersecurity Practices under Section 5 of the FTC Act

Robert A. Schwinger and Neal J. McLaughlin

17

When Backup Tapes Become Discoverable – A Costly Lesson in the Importance of Information Governance

Corey Lee and Meghan A. Podolny

22

Court of Justice of the European Union Declares EU Commission's U.S. Safe Harbor Decision Invalid

Romano F. Subiotto and Christopher J. Cook

25

In the Courts

Steven A. Meyerowitz

29

Legislative and Regulatory Developments

Steven A. Meyerowitz

34

Industry News

Victoria Prussen Spears

37

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 [3] (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 © 2016 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

(2016-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

RICHARD COHEN

Special Counsel, Kelley Drye & Warren LLP

CHRISTOPHER G. CWALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

DAVID C. LASHWAY

Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

AARON P. SIMPSON

Partner, Hunton & Williams 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 2016 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 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, 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.

When Backup Tapes Become Discoverable – A Costly Lesson in the Importance of Information Governance

*By Corey Lee and Meghan A. Podolny**

This article discusses a recent district court opinion that should caution all companies to be vigilant as to their email and document retention practices.

Companies should remember that their information governance practices may have significant financial repercussions if they become involved in litigation. One court in the District of Nevada recently took a novel approach to analyzing the accessibility of emails stored on backup tape. In *United States ex rel Guardiola v. Renown Health*,¹ the United States District Court for the District of Nevada opined that Renown's business practice of retaining email older than six months on backup tape foreclosed it from successfully arguing that the emails were shielded from discovery as not reasonably accessible because of burden or cost. The court also refused to shift to the requesting party the cost of restoration and review of the email at issue. A key element to this decision was the court's perception that Renown's email archival practices were out-of-date, and it also considered the use of backup tapes for recordkeeping without consideration to "the risk of litigation and corresponding discovery obligations" as indicative of a failure to "implement a sensible email retention policy." What is unique about this decision is that the court focused on Renown's business decisions on how to manage its information in the *absence* of pending discovery, and determined those pre-litigation business decisions were the critical factor to prevent the company from avoiding discoverability of documents archived per those decisions.

BACKGROUND

In this case, Renown opposed Relator's motion to compel production of email from a "gap period" during which, pursuant to Renown's email retention policy, emails older than six months were stored solely on backup tape prior to any duty to preserve documents. Renown argued that restoration of the backup tapes containing those emails would cost more than \$248,000, which would include data processing and contract review expenses, and that the restoration, review and production of email from tape with this price tag rendered that data inaccessible.

* Corey Lee is a partner at Hunton & Williams LLP focusing on commercial litigation and internal investigations. Meghan A. Podolny is an associate at the firm concentrating her practice on commercial litigation, information governance, and eDiscovery issues. The authors may be contacted at leec@hunton.com and mpodolny@hunton.com, respectively.

¹ No. 3:12-cv-00295-LRH-VPC (D. Nev. Aug. 25, 2015).

THE DISTRICT COURT'S DECISION

The court found an earlier line of case authority supporting the proposition that information stored on archival backup tapes is generally not reasonably accessible as “far from dispositive.” The court rejected the suggestion that data kept on backup tapes was inaccessible, particularly given today’s technology, stating “undue burden is fact specific and no format is inaccessible per se.” It instead analyzed whether the requested production constituted an undue burden or an undue cost. Because the restoration would be conducted by an outside vendor and utilize minimal resources within the company, the court found there was no burden placed on the company itself.

As to the question of undue cost, the court determined that only the cost of the physical restoration could be considered, and dismissed inclusion of related review and storage costs. Considering the physical restoration cost of approximately \$136,000, the court determined the restoration not unduly costly primarily for two reasons: (1) \$136,000 was a fraction of Renown’s annual revenues of \$2.6 billion and (2) Renown *elected* to use disaster recovery tapes to store archival data.

The court cited *Starbucks Corp. v. ADT Sec. Servs., Inc.*,² for the premise that a party cannot be relieved of its duty to produce documents merely because the party chose a means to preserve the evidence that makes ultimate production of relevant documents expensive. The court also cited the Sedona Conference, arguing that “[o]rganizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup tapes. They should not be used for record keeping.” In sum, the court held that to the extent a restoration cost of \$136,000 was attributable to Renown’s “failure to earlier implement a sensible email retention policy and its choice to use an archival/backup solution that did not maintain ESI in an indexed or otherwise searchable manner,” Renown bore the responsibility of the cost and it was not unreasonable.

Though finding the data reasonably accessible, the court nevertheless decided to consider the factors for whether good cause existed to order production under the balancing test of Federal Rule of Civil Procedure 26(b)(2)(B):

- (1) the specificity of the discovery request;
- (2) the quantity of information available from other and more easily accessed sources;
- (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
- (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
- (5) predictions as to the importance and usefulness of further information;

² No. 08-cv-900-JCC (W.D. Wash. Apr. 30, 2009).

- (6) the importance of the issues at stake in the litigation; and
- (7) the parties' resources.

Weighing each factor, the court concluded there was good cause for the discoverability of the emails on the backup tapes. The court then considered those same factors and found cost shifting was unwarranted.

Many courts would consider data kept on backup tapes as not reasonably accessible unless there was a showing that negligent or reckless action after the duty to preserve arose caused the data to be stored solely on archival media. This court, however, heavily focused on Renown's business decisions on how to manage its discovery *in the absence of pending litigation* as the justifying factor for causing the data to be discoverable. The opinion fails to discuss some important questions, including:

- whether data was regularly restored from backup tape for non-disaster recovery purposes;
- whether the emails sought could be considered records that should have been retained active in the company longer than six months under Renown's retention policy; and
- whether a more minimal approach would be appropriate, including sampling a portion of the tapes to confirm whether the communications sought by Relator would likely be contained in those email communications.

CONCLUSION

This aggressive approach by the court should caution all companies to be vigilant as to their email and document retention practices. The decisions that companies make to manage their information could prop them up for success or failure in handling litigation. Without proper guidelines to determine how data is organized, collected, and disposed of, companies may very well face a discovery dilemma like Renown. A data management strategy, carefully considered and employed, can proactively simplify the eDiscovery process, reducing those costs and reducing the risk of spoliation claims or litigating motions over archival data discoverability, while also helping to secure sensitive information.

This article presents the views of the authors and do not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed; readers should consult with legal counsel with respect to any legal advice they require related to the subject matter of the article.