AN A.S. PRATT PUBLICATION
OCTOBER 2020
VOL. 6 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 **NUMBER 8** **OCTOBER 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*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [245] (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. 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, 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, 630 Central Ave., New Providence, NJ 07974.

An Overview of Key Issues in Privacy and Cyber Litigation

By Tara L. Trifon and Hannah Oswald *

This article provides an overview of key issues in privacy and cybersecurity litigation.

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right "to be let alone."[1]

The 1890 article by Samuel Warren and Louis Brandeis in the Harvard Law Review, which includes the above quote, is widely regarded as the first American publication to advocate for a "right to be let alone." It highlighted the privacy invasions that result from "instantaneous photographs" and "numerous mechanical devices [that] threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"

The technological landscape has changed dramatically since 1890, but personal information still risks being "proclaimed from the [digital] house-tops." Indeed, as more of our private data is gathered, stored and disseminated electronically, it becomes increasingly likely that an unauthorized third party will get access to that information. That threat embodies the distinct but inherently connected principles of privacy and security, particularly cybersecurity. The growing ability to protect electronic information duels with the corresponding ability to steal the same.

Our legal framework is racing to keep up with these advances in two ways: (1) by applying already existing laws and claims to the issues raised by ever developing technologies and digital transformation, or (2) by enacting new laws and regulations. In either event, it is clear that privacy and cybersecurity litigation will continue and likely escalate. This article provides an overview of key issues to flag in such proceedings.

* Tara L. Trifon, a partner in the Hartford office of Locke Lord LLP, represents clients in complex disputes throughout the country with a specific focus on privacy and cybersecurity issues and financial services litigation. Hannah Oswald is an associate in the firm's Business Litigation & Dispute Resolution practice group in Chicago. The authors may be contacted at tara.trifon@lockelord.com and hannah.oswald@lockelord.com, respectively.

[1] Samuel Warren and Louis Brandeis, *The Right to Privacy,* 4 Harvard L.R. 193 (Dec. 15, 1890).

DOES THE PLAINTIFF HAVE STANDING TO SUE?

In order to have standing to bring any type of lawsuit, plaintiffs must be able to show that they have suffered a concrete injury that is traceable to the asserted wrongful action or inaction. Plaintiffs attempt to show such injury by alleging:

- Actual damages or harm;
- A reasonable fear of future damages; and
- Statutory damages.

Parties vigorously litigate a plaintiff's standing to pursue privacy and cyber claims, but the courts have not reached a consensus on how to rule on the issue. Litigants will focus on the facts and on the applicable law. They will also watch for further guidance by state and federal appellate courts, including the U.S. Supreme Court.

WHAT TYPES OF CLAIMS HAVE BEEN RAISED?

Many legal principles applied to privacy and cyber disputes are not new, but they are being applied differently to the current technology. Plaintiffs tend to bring claims sounding in:

- Tort (such as negligence);
- Contract (such as breach of contract) or quasi-contract (such as unjust enrichment); and
- Statutory violations (such as the California Consumer Privacy Act or the Illinois Biometric Privacy Act).

In addition, the boundaries of these doctrines will be tested even further as companies that already have access to some personal data start to expand into different industries (for instance, technology companies entering the health care industry).

WHAT ARE THE POSSIBLE DAMAGES?

If a case survives a motion to dismiss for lack of standing, the plaintiff may seek a variety of remedies including:

- Compensatory damages;
- Contractual or liquidated damages;
- Punitive damages;
- Statutory damages;

- Injunctive relief;
- Interest; and
- Reasonable attorney fees and costs.

The potential amount of damages can be daunting, particularly if the matter involves multiple plaintiffs or a certified class action.

IS THIS A CLASS ACTION?

Class actions may become more prevalent, raising complex issues such as:

- Impact of a class action being filed, including from a public relations perspective;
- Increased issues if a class is certified;
- Evidentiary issues; and
- Complicated settlement structures.

A critical hurdle in class action litigation is at the class certification stage, and the parties may expend a significant amount of time and resources during this process, particularly relating to factual and expert discovery. Additionally, while most of the privacy and cyber-related class actions settle, that process can be costly and complicated.

WHO IS RESPONSIBLE?

Because most, if not all, cases are resolved on a motion to dismiss or through settlement, there has not been much guidance on who can (or should) be held liable for the privacy and cyber claims. This raises a number of questions that should be considered during the litigation process:

- Was the correct party sued?
- Can the company be responsible (whether by contract, common law, or statute) for an employee or a vendor action or omission?
- Was the cyberattack a result of shortcomings in the company's administrative, technological or physical safeguards, or a misstep by the company's personnel or service providers, or was there a bad actor such that the incident could not reasonably have been prevented?
- What test or standard determines the adequacy or inadequacy of the company's administrative, technical, and procedural safeguards?

- Should the company consider filing a third party complaint to bring in new defendants and on what basis for each?

As privacy and cyber claims continue to be litigated, the universe of parties who may be held liable for these claims will continue to expand.

WHAT POSSIBLE CHALLENGES CAN ARISE DURING THE LITIGATION PROCESS?

The litigation process can be unwieldly, even for simple matters. This is only going to be exacerbated by the increasing complexity in the relevant technologies and subject matter. Some of the factual and legal challenges will include:

- Proving or disproving harm;
- Explaining technical aspects;
- Establishing the meaning of "reasonable security measures" given constant developments in available technology;
- Managing multiple parties, counsel, and agendas; and
- Handling multiple cases related to the same situation.

Preparedness for these challenges and the use of experts may help mitigate the risks.

WHAT SHOULD YOUR COMPANY DO AFTER A CYBER INCIDENT?

For matters arising out of a cyber incident, a lawsuit is usually filed quickly after the incident is disclosed, and therefore time is of the essence. Here are a few of the steps that your company may consider taking immediately upon discovering a potential cyber incidence and that may be appropriate to incorporate into its response plan:

- Consult with your insurer as appropriate;
- Engage experienced external counsel to lead the response;
- Consider attorney-client privilege and work product protection issues;
- Keep a record of all actions taken to mitigate the situation;
- Evaluate all legal, regulatory, and contractual notification requirements; and
- Consider scope of response as to legal, technical, crisis management, and public relations activities.

CONCLUSION

As more of our lives become dependent on technology, and as vulnerabilities in accessing personal data are exploited, it becomes increasingly likely that companies will become the target of a privacy or cyber related lawsuit. While it may not be possible to completely avoid litigation, being prepared and understanding the issues may improve your strategic options.