AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2015
VOL. 1 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 NUMBER 3 NOVEMBER/DECEMBER 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);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

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.

Privacy and Data Security In The Real World: You Can't Protect What You Don't See

By Thomas F. Zych*

If one does not know what information is gathered and used, who the users are and where the data actually go, the quality of advice and sufficiency of security programs are susceptible to foreseeable but unforeseen vulnerabilities. Asking the right questions from the outset is key. The author of this article suggests that sound counsel cannot commence until those involved have a solid understanding of exactly what the real, day-to-day data landscape looks like. These are the what, who, why, where, how long and what-now questions, the answers to which provide a sufficiently detailed map of the data used within the enterprise that requires appropriate security.

Information security is now a mature discipline. As with any mature discipline, the field has adopted and accepted conventional wisdom and standard approaches. With the passage of time and the accumulation of experience, we have a sufficient perspective on which to base a judgment as to how that wisdom and those approaches fit the world in which data really live and function.

ENSURING THE SECURITY OF PERSONAL AND PROPRIETARY INFORMATION

One way to assess and measure how we have come to approach ensuring the security of personal and proprietary information is to experience how *not* to go about it. In common practice, security counseling often breaks down into several principal tasks:

- Designing effective policies, procedures and practices for protecting sensitive information;
- Managing the security of information entrusted to third parties; and
- Implementing plans for responding to data security incidents.

For the lawyer, overlaying each of these elements is the appreciation and communication of compliance obligations and the consequences of security successes and failures. In other words, typical data security counseling usually focuses on the structure and articulation of security means – technical, administrative, and physical – that are bolted onto an enterprise's operations.

This approach, however, assumes that the information in question is fungible and exactly what we expect it to be, or at least that the data in question falls into predictable types (e.g., PHI, PII, proprietary information) that can be managed by

* Thomas F. Zych, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner in Thompson Hine LLP's Cleveland office, where he chairs the firm's Emerging Technologies practice and heads its Privacy & Cybersecurity team. He may be contacted at tom.zych@thompsonhine.com.

data classification almost without reference to the details of the enterprise's working environment. Even skilled privacy counsel may leave it to the enterprise to match its actual compliance to broadly articulated standards. Enterprises often contribute to the problem by seeking counsel's prior experience as a benchmark for best practices, using someone else's conclusions as a starting place for their own. Both of these approaches are inherently flawed. The core problem is they start one question too late.

WHAT IS THE CORRECT FIRST QUESTION?

What is the correct first question? I suggest that sound counsel cannot commence until those involved have a solid understanding of exactly what the real, day-to-day data landscape looks like. The best security plans, the best drafted security protocols and the tightest IT security systems will be inadequate unless all of the players first know exactly what data is at issue, where it resides and who can access it. Knowing that landscape requires greater insight than cataloging what types of information are at stake. Rather, no sound counsel will emerge until and unless the enterprise *and* its counsel develop a clear, documented and accurate picture of:

- The types of information each business function gathers, intentionally or otherwise, in the ordinary course of its business;
- Who within each function obtains, accesses and uses the information;
- Why the information is gathered and used, and whether it is used or accessed for reasons other than as originally intended;
- Where within the company's (1) IT systems, (2) physical storage and (3) individual users' enterprise and personal devices the information is accessed and stored;
- With whom outside the enterprise the information is shared, why and under what controls;
- How long information is *really* kept (notwithstanding published document retention policies) and how information is disposed of; and
- How real world, day-to-day business practices differ from existing policies and best practices.

These are the what, who, why, where, how long and what-now questions, the answers to which provide a sufficiently detailed map of the data used within the enterprise that requires appropriate security. The answers also give counsel an understanding of the real world of data practices around which practical and sustainable data security formulas can be built. The questions are pertinent to every type of information the enterprise uses.

Certainly, this approach is easily contrasted with the worst of all worlds: drive-by counsel. All of us have witnessed enterprises adopting stock policies in response to new data security laws or regulations to check off a compliance box – policies that often are

adopted but not really implemented. They are doomed from the start because they proscribe workplace information handling standards untethered to real business practices; they are only relevant by accident.

PERILS OF CONVENTIONAL SECURITY PLANNING AND ADVICE

But even a thoughtfully constructed information security framework risks ineffectiveness, or even irrelevance, if the information mapping step is skipped. If, for example, solid access and authentication systems are implemented regulating how and when employees may access a company's human resources information systems, the policy breaks down if the authorized employees regularly extract data, incorporate it into off-system spreadsheets, analyses and reports and email their work product to other company employees or even third-party service providers. In that scenario, the applicable rule works only as far as the understanding of how people *really* use information matches the articulated safeguard.

Another timely example further illustrates the point. A company's proprietary product formulations are stored in a research and development data storehouse, which only authorized users with dedicated user IDs and passwords may access. The company decides to use a data search utility (say, for example, a Google search appliance) to facilitate efficient data retrieval. Leaving aside the specifications and configuration of the utility, knowing that the utility is in use (or even that it is contemplated) allows counsel to calibrate the security rules to take into account this new access point and suggest controls on the use of the utility itself. On the other hand, ignorance of the new data retrieval capability may result in a facially adequate policy that falls prey to an unappreciated back door.

Let's consider one more example. A consumer products company operates a sophisticated customer relations system populated with robust and granular data about current and prospective buyers. The system is used for a wide variety of real-time – and perfectly lawful – communications in multiple media. The selection of data fields, the provisioning of limited access, the necessary controls to keep personal data on the system and the appropriate technical protections against intrusion all are in place. What could go wrong?

Perhaps this: Once in operation, the data storehouse becomes attractive for joint marketing efforts with channel partners. Let's assume that all privacy notices are sufficient to permit such sharing. Even so, the connection of an initially secure system to a system processing a new relationship raises three potentially serious security concerns. First, data are being transmitted from the protected system by a communication system of uncertain security. Second, the data are transferred to a partner's secured system, which may or may not meet the first enterprise's standards. Third, the second system may turn out to be a transit point to other enterprise and personal systems on the recipient's end. Remember, data persist and move. The benefits of all of

the careful planning on the front end, and the design and implementation of the original marketing database can be lost if the new collaborative use either was not anticipated up front or considered in an ongoing review of database use and the parties then fail to anticipate and plan for (or at least respond to) flexible uses of existing systems.

Each of these examples illustrates the perils of conventional security planning and advice. While it may sound naïve or heretical, data exist to serve business practices and not the other way around. It is tempting to assume that information is used only as originally designed, for the original purposes and only by those involved in the intended activities. That's just not how we work today. Information is critical to virtually every business activity, and "speed to know" is both an expectation and a competitive imperative. Business rewards quick and accurate use of data, and no one should be surprised when we look for relevant information where, when and how we need it.

OPTIONS

There are two choices in the face of this reality. First, a business may lock down data to only its originally intended uses and single storage locations. This approach has a surface attraction: safety. But this approach – not an uncommon one – is unlikely to survive real-world use. It presumes perfect foresight, it assumes all data types and their uses can be anticipated, and it concludes without review and reconsideration.

The second approach is to delay creating and implementing data security policies, protocols and procedures until a robust picture is created of what data really are gathered, used, stored and communicated throughout the organization. And there is one simple way to do this: Talk to the people who actually handle the information. Surely, sophisticated data mapping tools exist to provide detailed diagrams of how information is stored and communicated within a business's IT environment. These tools not only assist in identifying security vulnerabilities, they provide useful collateral benefits such as ESI gathering and protection in private litigation and government enforcement. But, by themselves they fail to reveal how real people use real information in real activities. Going to the horse's mouth remains the best way to learn how information really flows.

It is, of course, impossible to query every conceivable data user individually. However, covering the breadth of business franchises, selecting representative users senior enough to appreciate the full range of a function's operations while not being removed from day-to-day operations, and discussing what information is used, where it comes from and where and to whom it is communicated, will both highlight practical vulnerabilities and locate where controls are best applied. A parallel set of focused discussions with IT management and functional support allows the counselor to test actual use against system design, as well as system security adequacy against

real-world experience. These two paths should (in an ideal environment) proceed together, allowing cross-checking throughout the undertaking.

This exercise will provide a realistic evaluation of actual information practices upon which reliable security measures can be overlaid. Rather than a rules-based regime, best (or at least better) practices can be established and actual vulnerabilities of the type illustrated above can be identified and mitigated. Memorialized, the evaluation provides a way to predict vulnerabilities when new systems are implemented and as the business evolves. This initial evaluation also makes ongoing evaluation more efficient and focused.

CONCLUSION

In the end, how any enterprise approaches information security should be an individual decision. There are no real sizes when it comes to adequate information security, let alone a size that fits all. But one reliable constant remains across all businesses: If one does not know what information really is gathered and used, who the users are and where the data actually go, the quality of advice and sufficiency of security programs are susceptible to foreseeable but unforeseen vulnerabilities. Asking the right questions from the outset is key.