AN A.S. PRATT PUBLICATION
JUNE 2025
VOL. 11 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 5** **June 2025**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
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) 487-3385

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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

(2025–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, 631.291.5541. 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Tell Me Lies: The Legal Risks Associated with Misrepresenting Data Security and Privacy

By Starr Turner Drum, Sarah S. Glover and Noor K. Kalkat*

In this article, the authors explain that cybersecurity and privacy risk is an enterprise risk and must be addressed holistically and consistently.

U.S. companies public and private across all industry verticals have come to use representations about technology, including the company's data security and privacy practices, as a marketing tool. Before touting the ways in which a company protects its systems and customer data, however, organizations would be well advised to appreciate the potential pitfalls.

THE RISKS

There are myriad ways a business can be held accountable for failing to do what it tells a customer it will do. Failing to abide by promises – contractual or otherwise – to secure data could lead to breach of contract or fraud claims, customer churn and reputational damage. Businesses should also be aware that there are governing statutory schemes and regulatory enforcement precedent directly on point when it comes to making misrepresentations about an organization's data security and privacy practices and should take steps to stay on the right side of the law.

FTC ENFORCEMENT

The Federal Trade Commission (FTC) is empowered under Section 5 of the FTC Act to "prevent persons, partnerships or corporations" from using "unfair or deceptive acts or practices in or affecting commerce." Section 5 does not explicitly mention data security or privacy. However, the FTC has long maintained its authority to go after companies that misrepresent the way they protect customer data to the public. This authority has been challenged, but unsuccessfully. The FTC's action against Wyndham Worldwide Corp. in 2012 solidified the commission's enforcement authority in this domain.[1]

The FTC's complaint against Wyndham alleged that Wyndham failed to take reasonable security measures to safeguard personal information, which resulted in substantial consumer injury when hackers obtained unauthorized access to Wyndham's computer networks on three separate occasions. On interlocutory appeal to the U.S.

* The authors, attorneys with Polsinelli, may be contacted at sdrum@polsinelli.com, sglover@polsinelli.com and nkalkat@polsinelli.com, respectively.

[1] Complaint for Injunctive and Other Equitable Relief, FTC v. Wyndham Worldwide Corp. (D.N.J. 2012).

Court of Appeals for the Third Circuit, the court affirmed that the FTC has authority to regulate data security.

Since Wyndham, the FTC has pursued hundreds of data security and privacy actions under Section 5 across a number of industries, including against social media companies; application developers; data brokers; ed tech, ad tech and health tech companies; online retailers; and companies in the Internet of Things (loT) space. All these actions essentially boil down to one or two things: (1) You do not do what you say, and/or (2) You do not adequately protect data. Many findings have resulted in up to 10-figure penalties and 20-year consent decrees against companies the FTC has prosecuted.

What makes a data security or privacy statement "unfair" or "deceptive"? The FTC will know it when it sees it.[2] Companies are encouraged to heed lessons learned from prior enforcement actions. Here are noteworthy examples of actions prosecuted as unfair or deceptive by the FTC over the years:

- Failing to implement patch management policies and procedures to ensure timely remediation of critical security vulnerabilities and using obsolete (end-of-life (EOL)) versions of database and web server software;[3]
- Representing that the company provides end-to-end data encryption but failing to do so in certain instances;[4]
- Representing that the company uses standard security practices but failing to test or review security features and failing to conduct regular risk assessments, vulnerability scans and/or penetration testing of its networks and databases;[5]

[2] An act or a practice is "unfair" if:
(1) It causes or is likely to cause substantial injury to consumers;
(2) The injury is not reasonably avoidable by consumers; and
(3) The injury is not outweighed by benefits to consumers or competition.
A practice is "deceptive" if:
(1) A representation, omission or practice misleads or is likely to mislead the consumer;
(2) A consumer's interpretation of the representation, omission or practice is considered reasonable under the circumstances; and
(3) The misleading representation, omission or practice is material.

[3] In the Matter of CafePress, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter.

[4] In the Matter of Zoom Video Communications, Inc., available at https://www.ftc.gov/system/files/documents/cases/1923167zoomcomplaint_0.pdf.

[5] In the Matter of Drizly, available at https://www.ftc.gov/legal-library/browse/cases-proceedings/2023185-drizly-llc-matter.

- Failing to have a policy or procedure for inventorying and deleting consumers' personal data stored on the company's network;[6]
- Failing to protect consumer personal data in the ways stated in a company's online privacy policy;[7]
- Presenting misleading public-facing statements to consumers about the anonymity of browsing data collected and sold;[8]
- Retaining voice recordings after advising consumers that they had been deleted and could request deletion at any time;[9]
- Sharing personal health information with advertisers despite a privacy notice promise to never do so.[10]

The FTC has stated in the context of misleading and deceptive advertising that it does not pursue subjective claims or "puffery" – claims such as "this is the best hairspray in the world."[11] However, if there is an objective component to the claim, such as "more consumers prefer our hairspray to any other" or "our hairspray lasts longer than the most popular brands," then the company will need to make sure it has adequate substantiation before making the claim. This is especially true in the case of representations about data security and privacy because the consequences can be significant. If a hairspray company doesn't live up to the hype, consumers may experience frizz. If a company fails to protect personal data, consumers may experience identity theft.

SEC ENFORCEMENT

The FTC is not the only regulator to police this type of activity. The Securities and Exchange Commission (SEC) has recently flexed its muscle by bringing an enforcement action against SolarWinds Corp. and its chief information security officer (CISO) (collectively, the defendants) after SolarWinds sustained a massive supply chain attack in 2020 affecting its flagship security software platform.

The software was compromised after attackers injected malicious code into an application before it was put into operation at thousands of companies and government agencies.

---

[6] Id.

[7] In the Matter of Chegg, Inc., available at https://www.ftc.gov/system/files/ftc_gov/pdf/Chegg-Complaint.pdf.

[8] In the Matter of Avast Ltd. et al., available at https://www.ftc.gov/system/files/ftc_gov/pdf/202_3033_-_avast_final_consent_package.pdf.

[9] U.S. v. Amazon.com, Inc., available at https://www.ftc.gov/system/files/ftc_gov/pdf/1923128amazonalexaorderfiled.pdf.

[10] U.S. v. GoodRx Holdings, Inc., available at https://www.ftc.gov/system/files/ftc_gov/pdf/goodrxfinalstipulatedorder.pdf.

[11] Myths and Half-Truths About Deceptive Advertising (October 15, 1996), available at https://www.ftc.gov/news-events/news/speeches/myths-half-truths-about-deceptive-advertising.

The SEC alleged that the defendants "defrauded SolarWinds' investors and customers through misstatements, omissions and schemes that concealed both the Company's poor cybersecurity practices and its heightened – and increasing – cybersecurity risks."

Among other claims, the SEC alleged that SolarWinds made false and misleading statements in its public-facing website material as well as its press releases, blog posts and podcasts. Chiefly, SolarWinds maintained a "Security Statement" on its website that summarized its data security program – a not uncommon feature of many software and technology company websites. The SEC alleged that the following representations were revealed to be fraudulent in light of the cyberattack:

(1) That SolarWinds adhered to the National Institute of Standards and Technology (NIST) Cybersecurity Framework;

(2) That the company developed its software using a secure software development life cycle (SSDLC); and

(3) That the company implemented and maintained adequate network monitoring, password protocols and access controls.

The SEC alleged that the defendants knew the company had experienced "widespread and persistent failures" in each of these security areas that went to the heart of its products as a security company, thereby making them material to investors.

The backlash to the SEC's claims has been loud – industry experts and practitioners are concerned about a "chilling effect" on the dissemination of information about security and privacy, and especially on the ability of CISOs and other technology leaders to adequately perform their jobs for fear of being held personally responsible for a data security incident.

LITIGATION

Privacy- and cybersecurity-focused litigation has skyrocketed during the past few years. Between 2021 and 2023, the volume of complaints referencing "ransomware" increased by more than 600% and the volume of complaints referencing "data breach" increased by more than 200%. These lawsuits will often fold in consumer protection claims that allege defendants made misrepresentations about how they would treat personal information.[12]

The more explicit companies are about the ways in which they will safeguard consumer information, the more fodder for the plaintiffs' bar when those protections fail. What may have initially seemed like a great, marketing-focused commitment to safeguard consumer personal data can quickly become a pre-written checklist of security and privacy commitments that the organization allegedly failed to honor.

[12] Myths and Half-Truths About Deceptive Advertising (October 15, 1996), available at https://www.ftc.gov/news-events/news/speeches/myths-half-truths-about-deceptive-advertising.

THE GUIDANCE

It goes without saying that any contractual requirements regarding data security and privacy should be thoroughly reviewed by the appropriate legal and technical subject matter experts. Most companies, however, do not deploy the same level of diligence when it comes to marketing and other public-facing material about data security and privacy – and they need to, in light of the authority cited above.

There are a number of stakeholders across an organization that may touch or weigh in on public-facing representations about data security and privacy – marketing, legal/compliance, IT/security, customer relations, product development, etc. Businesses need to deploy adequate review and approval protocols across these stakeholders to govern any statements about the organization's data security and privacy practices. Failure to do so can result in the unintentional and/or negligent publication of false and misleading statements that introduce legal risk to the organization. Below are action items and guidelines to help reduce this risk:

- Develop a website content development policy and procedure.
- When selecting material (existing or new) for the website, accuracy trumps everything else.
- Avoid unqualified statements that leave no room for exceptions. Most organizations could not stand by the bald statement "We encrypt all data" without qualification.
- Avoid absolutes. Companies should always avoid using the word "always" in this content and should never use the word "never."
- Avoid guarantees. There are no guarantees when it comes to data security and privacy. You cannot "100% guarantee" that you can keep data secure – nobody can or should make this representation.
- Don't make promises you can't keep. For example, don't tell customers you will delete their data upon request or within 30 days following termination if your organization has not deployed adequate protocols to reasonably ensure that this in fact happens.
- Less is more. Detailed technical details are inappropriate for public-facing marketing content. Save that for product specs and terms and conditions.
- Public-facing information about data security and privacy must be reviewed by legal and compliance subject matter experts.

- Public-facing information about data security and IT must be reviewed by the internal IT subject matter experts as well.
    - Note that a company's IT systems and security controls change frequently – what was true two years ago may no longer be accurate. The regular review of existing content – not just net new content – is important.
- Legal and marketing professionals alike know that terminology matters and descriptive words should be chosen carefully.
    - For example, if you state that your company deploys "military grade" security, that could be misinterpreted as erroneously implying that a company's products are compliant with federal defense contracting standards (e.g., the Federal Acquisition Regulations System/Defense Federal Acquisition Regulation Supplement).

THE TAKEAWAY

Ten-plus years ago, touting your strong cybersecurity and privacy practices may have been a market differentiator. Today, keeping data secure and upholding well-established privacy principles is table stakes. Organizations that do not do what they say they do can and will be held accountable – by their customers, by their industry, by the plaintiffs' bar and by regulators. As with cybersecurity and privacy generally, this is not just a marketing issue or an IT issue or a legal issue. Cybersecurity and privacy risk is an enterprise risk and must be addressed holistically and consistently.