AN A.S. PRATT PUBLICATION
JANUARY 2026
VOL. 12 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 1** **January 2026**

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

(2026–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.

Beyond the Perimeter: Securing OAuth Tokens and API Access to Thwart Modern Cyber Attackers

By L. Judson Welle and Victoria F. Volpe*

OAuth tokens streamline access but create new vulnerabilities that threat actors are exploiting. The authors of this article discuss how to secure token infrastructure through robust monitoring, governance, and vendor management.

The threat landscape continues to evolve, and cybersecurity professionals must keep pace with threat actors' changing tactics and objectives. A recent supply attack that reportedly affected hundreds of companies shows an increased focus by attackers on stealing and abusing OAuth tokens and other secrets to gain programmatic access to companies' cloud environments. The lesson from this is that modern cyber hygiene is no longer just about securing your company's perimeter – it also requires vigilant monitoring of the access pathways within its digital ecosystem.

UNDERSTANDING OAUTH TOKENS: CONVENIENCE WITH RISK

OAuth tokens enable users to navigate between applications using a single log-on, creating a more seamless user experience. For example, a user may log on to Microsoft 365 using their credentials and multi-factor authentication (MFA). The resulting OAuth token allows the user to access other connected applications while bypassing repeated MFA prompts. This approach reduces credential theft risk by eliminating the need to log on to each application separately.

Tokens can also be configured to provide granular access controls to specific resources, activities, and data. However, if not managed and monitored properly, OAuth tokens become attractive targets for threat actors.

THE HIDDEN VULNERABILITIES OF OAUTH IMPLEMENTATIONS

Several common misconfigurations and oversight gaps make OAuth tokens vulnerable to exploitation:

- *Excessive Permissions*: Many tokens are configured with overly broad permissions – such as the ability to read all emails, create new users, or modify sensitive data – far exceeding what users actually need to perform their roles.

* The authors are attorneys at Goodwin Procter LLP. They may be contacted at jwelle@goodwinlaw.com and vvolpe@goodwinlaw.com, respectively.

- *Extended Session Duration*: Tokens that remain valid for extended periods create larger windows of opportunity for attackers. Once stolen, these long-lived tokens can be exploited for weeks or even months.
- *Insufficient Monitoring*: Without robust monitoring for unusual activity – such as unexpected application programming interface (API) calls, high-volume downloads, or access from suspicious IP addresses – token abuse can persist undetected while threat actors conduct reconnaissance and exfiltrate data.
- *Limited Native Detection Capabilities*: Many platforms have limited built-in abilities to configure comprehensive token monitoring without additional tools or specialized licensing, leaving organizations unaware of potential abuse.
- *Inadequate Key Protection*: OAuth secrets and refresh tokens stored in development environments, repositories, or configuration files are often inadequately protected, creating opportunities for theft.

BUILDING A COMPREHENSIVE OAUTH SECURITY STRATEGY

Organizations seeking to leverage the benefits of OAuth tokens while mitigating risks should implement a multilayered security approach:

1. *Establish Strong Governance and Policies*
    - *Define Token Life Cycle Management*: Assign clear responsibility for token creation, review, renewal, and revocation. Establish policies for the maximum token lifespan based on its risk level.
    - *Implement Least-Privilege Principles*: Configure tokens with the minimum permissions necessary to accomplish specific tasks. Regularly review and adjust scopes as roles and responsibilities evolve.
    - *Document Token Inventory*: Maintain a comprehensive register of all OAuth applications, permissions, and business justifications.
2. *Deploy Technical Controls and Monitoring*
    - *Enable Advanced Monitoring Tools*: Implement or configure tools that can detect and alert on suspicious activity, including:
        - Unusual API call patterns or frequencies.
        - High-volume data downloads.
        - Access from unexpected geographic locations or IP addresses.

- Token usage outside normal business hours.
- Attempts to escalate privileges.

- *Secure Token Storage*: Protect OAuth secrets and refresh tokens with encryption, access controls, and secrets management solutions. Never store tokens in publicly accessible repositories or configuration files.
- *Implement Token Rotation*: Establish automated token rotation schedules, particularly for high-privilege tokens. Shorter token lifespans reduce the windows of opportunity for attackers.
- *Configure Conditional Access Policies*: Layer additional authentication requirements for high-risk scenarios, such as access from new devices or unusual locations.

3. *Strengthen Vendor and Third-Party Risk Management*

- *Conduct OAuth-Specific Vendor Assessments*: When evaluating third-party vendors, assess their OAuth implementation practices, including:
  - How they store and protect OAuth secrets.
  - Their token monitoring and anomaly detection capabilities.
  - Their incident response procedures for token compromise.
  - The scope of permissions they request.
- *Prioritize High-Risk Vendors*: Focus initial assessments on vendors with the highest level of access to sensitive data, then work systematically through vendors with lower access levels.
- *Review and Minimize Vendor Permissions*: Regularly audit the permissions granted to third-party applications. Revoke access for unused applications and reduce permissions for others if possible.
- *Establish Contractual Protections*: Include specific OAuth security requirements in vendor contracts, along with notification obligations in the event of token compromise.

4. *Build Detection and Response Capabilities*

- *Develop Token Compromise Playbooks*: Create specific incident response procedures for suspected OAuth token theft, including:

- Immediate token revocation processes.
- User notification and reauthentication requirements.
- Forensic analysis procedures to determine the compromise's scope.
- Communication protocols for affected stakeholders.

- *Conduct Regular Security Testing*: Include OAuth security in penetration testing and red team exercises. Test your company's ability to detect token theft and abuse.
- *Train Security Teams*: Ensure security operations center analysts understand OAuth-specific attack patterns and know how to investigate suspicious token activity.

5. *Expand Perimeter Security to Edge Devices*

The proliferation of edge devices – including Internet of Things sensors, mobile devices, and remote access points – has created additional attack vectors that threat actors increasingly exploit. OAuth tokens accessed from compromised edge devices can provide attackers with footholds into enterprise systems.

- *Implement Edge Device Security Controls*: Deploy endpoint detection and response solutions on all devices that access OAuth-enabled applications. Ensure edge devices meet minimum security standards before granting access.
- *Monitor Edge Device Behavior*: Track authentication patterns from edge devices for anomalies, such as simultaneous log-ons from geographically distant locations or unusual data access patterns.
- *Segment Network Access*: Limit what edge devices can access within your company's network. Apply zero-trust principles to ensure compromised edge devices can't freely move laterally.

MOVING FORWARD: AN EVOLUTION IN SECURITY MINDSET

OAuth security requires organizations to evolve their perimeter-focused security model into one that also assumes threats may already be inside their networks. By implementing comprehensive governance, deploying robust monitoring, strengthening vendor management, building detection and response capabilities, and extending security to edge devices, organizations can leverage the benefits of OAuth while significantly reducing their risk exposure.

Attack trends and recent incidents serve as reminders that OAuth security is not just an internal concern – it is also a supply chain issue that affects entire ecosystems of interconnected organizations. Proactive measures today can prevent costly breaches tomorrow.