AN A.S. PRATT PUBLICATION
FEBRUARY-MARCH 2023
VOL. 9 NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: IT'S A PRIVILEGE
Victoria Prussen Spears

U.S. SUPREME COURT TO DECIDE WHEN ATTORNEY-CLIENT COMMUNICATIONS THAT CONTAIN "HYBRID" LEGAL AND BUSINESS ADVICE ARE PROTECTED BY THE ATTORNEY-CLIENT PRIVILEGE
Erik Snapp, Andrew S. Boutros, Jacqueline Harrington, Christina Guerola Sarchio and Jay Schleppenbach

NEW EXECUTIVE ORDER DETAILS NATIONAL SECURITY FACTORS TO BE CONSIDERED BY THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES
Paul T. Luther, Alexander P. Reinert, Cullen Richardson and Matthew T. West

FEDERAL COMMUNICATIONS COMMISSION RELEASES ITEM AMENDING EQUIPMENT AUTHORIZATION RULES TO PROTECT U.S. NATIONAL SECURITY
Megan L. Brown, Scott D. Delacourt, Kathleen E. Scott, Joshua S. Turner, Sara M. Baxenberg and Kelly Laughlin

FEDERAL TRADE COMMISSION SETTLES WITH DRIZLY FOR ALLEGED SECURITY FAILURES
Alexander G. Brown, Kathleen Benway and Ashley Miller

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES PROPOSES UPDATED CYBERSECURITY REGULATION
John P. Carlin, Roberto J. Gonzalez, Steven C. Herzog and Cole A. Rabinowitz

CALIFORNIA EXPANDS ITS CONFIDENTIALITY OF MEDICAL INFORMATION ACT TO REGULATE MENTAL HEALTH DIGITAL SERVICES
Sharon R. Klein, Alex C. Nisenbaum, Jennifer J. Daniels and Karen H. Shin

PREPARING FOR TODAY, AND FOR THE FUTURE, IN CALIFORNIA
Devika Kornbacher

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 2** **February-March 2023**

Editor's Note: It's a Privilege
Victoria Prussen Spears 37

U.S. Supreme Court to Decide When Attorney-Client Communications That Contain "Hybrid" Legal and Business Advice Are Protected by the Attorney-Client Privilege
Erik Snapp, Andrew S. Boutros, Jacqueline Harrington, Christina Guerola Sarchio and Jay Schleppenbach 39

New Executive Order Details National Security Factors to Be Considered by the Committee on Foreign Investment in the United States
Paul T. Luther, Alexander P. Reinert, Cullen Richardson and Matthew T. West 44

Federal Communications Commission Releases Item Amending Equipment Authorization Rules to Protect U.S. National Security
Megan L. Brown, Scott D. Delacourt, Kathleen E. Scott, Joshua S. Turner, Sara M. Baxenberg and Kelly Laughlin 47

Federal Trade Commission Settles with Drizly for Alleged Security Failures
Alexander G. Brown, Kathleen Benway and Ashley Miller 52

New York State Department of Financial Services Proposes Updated Cybersecurity Regulation
John P. Carlin, Roberto J. Gonzalez, Steven C. Herzog and Cole A. Rabinowitz 56

California Expands Its Confidentiality of Medical Information Act to Regulate Mental Health Digital Services
Sharon R. Klein, Alex C. Nisenbaum, Jennifer J. Daniels and Karen H. Shin 62

Preparing for Today, and for the Future, in California
Devika Kornbacher 65

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [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

(2023–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 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.

New Executive Order Details National Security Factors to Be Considered by the Committee on Foreign Investment in the United States

By Paul T. Luther, Alexander P. Reinert, Cullen Richardson and Matthew T. West*

In this article, the authors explain that U.S. companies in certain industries and business sectors that are contemplating raising capital from foreign sources, or that are engaging in mergers and acquisitions transactions involving foreign parties, should expect that these activities will be subject to heightened regulatory scrutiny from the Committee on Foreign Investment in the United States.

President Joe Biden has signed an executive order (EO)[1] detailing key factors for the Committee on Foreign Investment in the United States (CFIUS or the Committee) to consider when reviewing transactions for national security risks. The EO provides direction to CFIUS by elaborating on existing statutory factors and adding five sets of national security factors for CFIUS to consider during its review process.

Moreover, the EO highlights for CFIUS specific industry sectors that have national security implications, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements), and elements of the agricultural industrial base.

Importantly, the EO does not alter existing CFIUS processes or legal jurisdiction. Although CFIUS already focuses on many of the factors articulated in the EO, the EO provides explicit direction to CFIUS that arguably formalizes the Committee's recent approach to national security reviews. However, in the long term, these new factors may provide a basis for a gradual expansion of CFIUS's purview and they signal to market participants what types of inbound investment may raise national security concerns.

In a statement,[2] the White House emphasized the importance of updating the foreign investment review process to remain responsive to evolving national security threats

---

* The authors, attorneys at Baker Botts L.L.P., may be contacted at paul.luther@bakerbotts.com, alexander.reinert@bakerbotts.com, cullen.richardson@bakerbotts.com and matthew.west@bakerbotts.com, respectively.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

[2] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

and noted that these new factors reflect the Biden Administration's overall national security priorities, which include "preserving U.S. technological leadership, protecting Americans' sensitive data, and enhancing U.S. supply chain resilience."

The EO directs the Committee to consider five specific sets of factors in its national security reviews of transactions that are subject to its jurisdiction (commonly referred to as "covered transactions"). Such transactions include (i) "covered control transactions" (i.e., any transaction with a foreign person that could result in control of a U.S. business by a foreign person), and (ii) "covered investments" (i.e., non-controlling investments that afford a foreign person (1) access to material, nonpublic technical information, (2) membership or observer rights on the board of directors, or (3) involvement in certain substantive decision-making in a U.S. business that is involved with critical technologies, critical infrastructure, or sensitive personal data).

1. RESILIENCE OF CRITICAL U.S. SUPPLY CHAINS

First, the EO states that the Committee should consider how a transaction will affect the resilience of critical U.S. supply chains that may have national security implications, including those outside of the defense industrial base. Foreign investment that shifts ownership, rights, or control to a foreign person in certain manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security may make the United States vulnerable to future supply disruptions of critical goods and services.

The EO states that the Committee should consider a covered transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base. These considerations include the degree of diversification through alternative suppliers across the supply chain, including suppliers located in allied or partner countries; supply relationships with the U.S. government; and the concentration of ownership or control by the foreign person in a given supply chain.

2. U.S. TECHNOLOGICAL LEADERSHIP

Second, the EO directs CFIUS to consider the effect on U.S. technological leadership in sectors affecting U.S. national security, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, climate adaptation technologies, and elements of the agricultural industrial base that have implications for food security.

The EO specifically identifies these sectors as fundamental to U.S. technological leadership and, therefore, national security. The Committee is instructed to consider whether a covered transaction involves manufacturing capabilities, services, critical mineral resources, or technologies in such sectors.

3. CUMULATIVE INVESTMENT TRENDS OF FOREIGN INVESTORS

Third, the EO directs the Committee to examine broader industry investment trends that may have consequences for a given transaction's impact on U.S. national security. Certain investments by the same foreign person in a sector or technology may appear to pose a limited threat when viewed in isolation, but when viewed in the context of previous transactions, it may become apparent that such investments can facilitate sensitive technology transfer in key industries or otherwise harm national security. For example, there may be a comparatively low threat associated with a foreign company or country acquiring a single firm in a sector, but a much higher threat associated with a foreign company or country acquiring multiple firms within the sector.

4. CYBERSECURITY RISK

Fourth, CFIUS will consider cybersecurity risks that threaten to impair national security. Investments by foreign persons with the capability and intent to conduct cyber intrusions or other malicious cyber-enabled activity may pose a risk to national security. This includes cyber actions intended to alter election outcomes, critical infrastructure, or the integrity or availability of communications. The EO directs CFIUS to consider whether a covered transaction may provide a foreign person, or their relevant third-party ties, with access to conduct such activities.

5. RISKS TO U.S. PERSONS' SENSITIVE DATA

Fifth, the EO calls out the continued national security risks associated with U.S. persons' sensitive data. The EO notes that technological advances have made possible re-identification or de-anonymization of what once was unidentifiable data.

Consequently, the EO directs CFIUS to consider potential risks posed by foreign persons who might exploit access to certain data on U.S. persons to target individuals or groups within the United States to the detriment of national security.

CONCLUSION

These factors indicate where additional CFIUS attention is likely to be directed in the near future, and they offer insight that can better inform the risks associated with cross-border investments, particularly in those industry sectors experiencing increased amounts of foreign investment.

Consequently, U.S. companies in these industries and business sectors that are contemplating raising capital from foreign sources, or that are engaging in mergers and acquisitions transactions involving foreign parties, should expect that these activities will be subject to heightened regulatory scrutiny from CFIUS.