AN A.S. PRATT PUBLICATION
SEPTEMBER 2024
VOL. 10 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 7** **September 2024**

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

(2024–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.

U.S. Commerce Department Issues Final Determination of Russia-Backed Cybersecurity, Antivirus Software

By Andrew K. McAllister, Robert A. Friedman, Noah Curtin and Ronnie Rosen Zvi*

In this article, the authors discuss a final determination by the U.S. Commerce Department's Office of Information and Communications Technology and Services banning Russian-backed cybersecurity firm Kaspersky Lab Inc. and its affiliates, subsidiaries and parent companies from, directly or indirectly, providing antivirus software and cybersecurity products or services in the United States or to U.S. persons.

The U.S. Department of Commerce's Office of Information and Communications Technology and Services (OICTS) within the Bureau of Industry and Security (BIS) has issued a final determination (Final Determination), pursuant to Executive Order (E.O.) 13873, "Securing the Information and Communications Technology and Services Supply Chain."[1]

The Final Determination bans Russian-backed cybersecurity firm Kaspersky Lab Inc. and its affiliates, subsidiaries and parent companies (collectively, Kaspersky) from, directly or indirectly, providing antivirus software and cybersecurity products or services in the United States or to U.S. persons. Violations of the Final Determination can result in civil and criminal penalties.

This Final Determination is the first of its kind issued pursuant to the E.O. and showcases the U.S. government's heightened scrutiny of supply chain security and over transactions involving sensitive technologies from "foreign adversaries," which is defined to include China, Cuba, Iran, North Korea, Russia and the Maduro Regime (Venezuela).[2]

BACKGROUND

On May 15, 2019, then-President Donald Trump signed into effect E.O. 13873, authorizing the Commerce Department to review certain transactions involving information and communications technology or services (ICTS) designed, developed, manufactured or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of a "foreign adversary" that pose an undue or acceptable risk to the United States or U.S. persons.

---

* Andrew K. McAllister (andrew.mcallister@hklaw.com) and Robert A. Friedman (robert.a.friedman@hklaw.com) are partners in the Washington, D.C., office of Holland & Knight LLP. Noah Curtin was a summer associate at the firm. Ronnie Rosen Zvi is an international law clerk at the firm.

[1] https://www.federalregister.gov/documents/2024/06/24/2024-13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc.

[2] See 15 C.F.R. 7.4(a)(5), available at https://www.ecfr.gov/current/title-15/subtitle-A/part-7/subpart-A/section-7.4#p-7.4(a)(5).

E.O. 13873, as implemented in 15 C.F.R. Part 7,[3] allows the Commerce Department to prohibit any person from acquiring, importing, transferring, installing, dealing in or using ICTS from a person owned by, controlled by or subject to the jurisdiction or direction of "foreign adversaries" where the Commerce Department determines the transaction:

(1) Poses an undue risk of sabotage to or subversion of ICTS in the United States;

(2) Poses an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the digital economy of the United States; or

(3) Poses an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

Prior to this action against Kaspersky, the Commerce Department had not taken any action pursuant to this authority.

BIS ACTION AGAINST KASPERSKY

What Is Kaspersky?

Kaspersky Lab Inc. is a U.S. subsidiary of a Russia-backed antivirus software and cybersecurity company. Key aspects of its business (software design, development and supply) are conducted in Russia. Additionally, Eugene Kaspersky – the company's founder, majority owner and current chief executive officer – is a Russian national who resides in Russia. From this information, the Commerce Department determined that Kaspersky is subject to the jurisdiction and direction of the Russian government, a "foreign adversary" per 15 C.F.R. 7.4(a)(5).

BIS Investigation and Review

On August 25, 2021, the U.S. Department of Justice (DOJ) referred Kaspersky's ICTS transactions involving the provision of cybersecurity and antivirus software and related services to persons subject to U.S. jurisdiction to the Commerce Department. Following its review of all relevant documents, the Commerce Department issued an Initial Determination on October 5, 2023, that was challenged by Kaspersky in its official written response. The Commerce Department ultimately rejected Kaspersky's challenge, including proposed mitigation measures, and announced the present Final Determination.

BIS found five key risks that Kaspersky's ICTS offerings pose to U.S. national security and to the safety and security of U.S. persons:

- Russia is a foreign adversary that continues to threaten the United States;
- Kaspersky is subject to the jurisdiction, control or direction of the Russian government;

- Kaspersky software provides the Russian government access to sensitive U.S. customer information;
- Kaspersky software allows for the capability and opportunity to install malicious software and withhold critical updates; and
- The manipulation of Kaspersky software, including in U.S. critical infrastructure, can cause significant risks of data theft, espionage and system malfunction.

It can also risk U.S. economic security and public health, resulting in injuries or loss of life.

Prohibitions on Kaspersky ICTS Software

According to the Final Determination, there are three sets of ICTS transactions that are restricted:

- ICTS transactions involving any cybersecurity product or service designed, developed, manufactured or supplied, in whole or in part, by Kaspersky, to include those products and services listed in Appendix B to the Final Determination.[4]
- ICTS transactions involving any antivirus software designed, developed, manufactured or supplied, in whole or in part, by Kaspersky to include those products and services listed in Appendix B.
- ICTS transactions involving the integration of software designed, developed, manufactured or supplied, in whole or in part, by Kaspersky into third-party products or services (e.g., "white-labeled" products or services).

Effective 12 a.m. EDT on July 20, 2024, Kaspersky is prohibited from entering into any new agreements with U.S. persons involving any one or more covered ICTS transactions identified above.

Additionally, effective 12 a.m. EDT on September 29, 2024, the Final Determination prohibits Kaspersky and any of its successors or assignees from providing antivirus signature updates and codebase updates associated with the ICTS transactions identified above, as well as operating the Kaspersky Security Network within the United States or on any U.S. person's information technology system. Furthermore and also effective at 12 a.m. EDT on September 29, 2024, the Final Determination prohibits the resale of Kaspersky cybersecurity or antivirus software, integration of Kaspersky cybersecurity or antivirus software into other products and services, along with licensing of Kaspersky cybersecurity or antivirus software for purposes of resale or integration into other products or services.

[4] https://oicts.bis.gov/pdfs/AppendixB.pdf.

ASSOCIATED ACTIONS AGAINST KASPERSKY BY BIS AND OFAC

Additions to the Entity List

Concurrently with the issuance of its Final Determination, BIS has also issued a Final Rule[5] amending the Export Administration Regulations (EAR) by adding three new entries to the Entity List.[6] The Entity List identifies entities believed to be involved in activities contrary to the national security or foreign policy interests of the United States and imposes additional licensing requirements for the export, reexport and transfer (in-country) of items subject to the EAR to listed entities.

The Final Rule, effective immediately, announced the addition of AO Kaspersky Lab and OOO Kaspersky Group in Russia, as well as Kaspersky Labs Limited in the United Kingdom, to the Entity List. According to the Final Rule, the reason for the addition of these entities is due to their cooperation with Russian military and intelligence authorities in support of the Russian government's cyber intelligence objectives.

OFAC Sanctions

On June 21, 2024 – the day following the issuance of the Final Determination – the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated 12 individuals[7] in executive and senior leadership roles at AO Kaspersky Lab (Russia) onto its Specially Designated Nationals and Blocked Persons List (SDN List) for operating in the technology sector of the Russian Federation economy.

As a result of the designation, U.S. persons are prohibited from engaging in transactions involving designated individuals or their property, including any entities that are owned, directly or indirectly, 50 percent or more by one or more designated individuals.

IMPLICATIONS

To provide time for Kaspersky's software customers to transition to alternative cybersecurity and antivirus software services, BIS is allowing Kaspersky to continue providing services to U.S. persons until September 29, 2024. Until that date, Kaspersky is permitted to provide antivirus software updates and codebase updates to current U.S. subscribers and users of its cybersecurity and antivirus products and services. However, effective July 20, 2024, Kaspersky will be prohibited from entering into any new agreements with U.S. persons involving covered products.

---

[5] https://public-inspection.federalregister.gov/2024-13695.pdf.

[6] https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744.

[7] https://home.treasury.gov/news/press-releases/jy2420.

Organizations and individuals looking to remove Kaspersky software from their internal systems and personal devices may review the Cybersecurity and Infrastructure Security Agency's (CISA) Software Removal Guide and Software Removal Guide[8] for Personal Devices,[9] respectively.

Additionally, companies that sell hardware or software containing embedded antivirus and cybersecurity software should ensure their products do not contain any Kaspersky software prohibited by the Final Determination. Companies should be aware that integrating or licensing Kaspersky cybersecurity or antivirus software into other products and services will be prohibited starting on Sept. 29, 2024. Note that any violation of the Final Determination may subject the violator to civil – and even criminal – penalties under the authority of the International Emergency Economic Powers Act (IEEPA), the same authority that applies to penalties under most economic sanctions programs.

Moreover, considering the potential exposure of sensitive data to malign actors and the potential lack of cybersecurity coverage, companies are encouraged to transition to alternative suppliers, since individuals or businesses that continue to use Kaspersky products would assume the risks of doing so.

Finally, U.S. persons should avoid engaging in any transactions involving the 12 designated individuals from Kaspersky leadership, and exporters dealing with items subject to the EAR should be aware of the addition of the three key Kaspersky entities to the Entity List and ensure they are not exporting covered items in cases where any of the entities are a party to the transaction.

IN SUMMARY

- The U.S. Department of Commerce has issued a Final Determination prohibiting Kaspersky Lab Inc., the U.S. subsidiary of a Russia-backed antivirus software and cybersecurity company, from providing antivirus software and cybersecurity products or services in the United States or to U.S. persons.
- This action is the first Final Determination issued by the Commerce Department's Office of Information and Communications Technology and Services (OICTS) and reflects the U.S. government's heightened scrutiny of supply chain security and transactions with "foreign adversaries" involving sensitive technologies.
- U.S. individuals and businesses that utilize Kaspersky software are strongly encouraged to transition to new cybersecurity and antivirus software suppliers for their products to avoid business disruption and/or violation of the Final Determination.

[8] https://www.cisa.gov/sites/default/files/2024-03/CEG_Software_Removal_Guide1_TLP_CLEAR_508c.pdf.

[9] https://www.cisa.gov/sites/default/files/2024-03/CapacityEnhancementGuide-GuideforPersonalDevices1_508c.pdf. GuideforPersonalDevices1_508c.pdf.

- In addition to the Final Determination, the Commerce Department's Bureau of Industry and Security (BIS), along with the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), carried out additional measures aimed at preventing transactions with, and exports of controlled items to, certain Kaspersky senior leadership officials and entities.

CONCLUSION

This Final Determination issued by the Commerce Department reflects the broader trend of increased enforcement of cross-border transactions involving U.S. persons and foreign adversaries. This new enforcement mechanism – carried out through BIS and OICTS, along with associated actions carried out by BIS and OFAC – reflects the Biden Administration's "whole of government" approach to combatting adversarial countries and protecting U.S. national security, with particular focus on data privacy of U.S. persons and U.S. critical infrastructure. Therefore, it is reasonable to expect additional measures and determinations of this nature to be issued in the near future.