AN A.S. PRATT PUBLICATION
NOVEMBER - DECEMBER 2023
VOL. 9 NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 9** **November - December 2023**

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
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*, [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.

Federal Communications Commission Kicks Off Voluntary IoT Security Label Program With Big Notice of Proposed Rulemaking

By Sara M. Baxenberg, Megan L. Brown, Kathleen E. Scott, Joshua S. Turner and Boyd Garriott*

In this article, the authors discuss a recent Notice of Proposed Rulemaking issued by the Federal Communications Commission in which the agency takes a broad view of its authority to enact a cybersecurity labeling regime for Internet of Things devices.

In a new Notice of Proposed Rulemaking (NPRM),[1] the Federal Communications Commission (FCC or Commission) imposes a short comment deadline for a complex new cybersecurity labeling regime for Internet of Things (IoT) devices. The NPRM also reveals that the agency – which traditionally has not regulated in the area of cybersecurity – is taking a broad view of its authority to enact this program.

At a high level, the NPRM proposes that participating entities will be able to display a Commission-created "IoT cybersecurity label" on their connected devices (the U.S. Cyber Trust Mark),[2] indicating conformance with "widely accepted cybersecurity standards." Although other parts of the federal government have considered IoT security and labeling issues, this cybersecurity labeling program would be a first for the FCC. The complexity of the NPRM raises important issues for stakeholders to consider, on a compressed timeline: initial comments were due by October 9, 2023 and reply comments by November 10, 2023.

The FCC's proposal is part of a White House initiative on IoT security, which recently kicked off. While the joint White House-FCC labeling initiative is new, it follows several years of work in this area, including guidance documents and pilot programs[3] by the National Institute of Standards and Technology (NIST) pursuant to a 2021 Executive Order on Improving the Nation's Cybersecurity (14028)[4] and direction from Congress,[5]

---

* The authors, attorneys with Wiley Rein LLP, may be contacted at sbaxenberg@wiley.law, mbrown@wiley.law, kscott@wiley.law, jturner@wiley.law and bgarriott@wiley.law, respectively.

[1] https://docs.fcc.gov/public/attachments/FCC-23-65A1.pdf.

[2] https://www.fcc.gov/cybersecurity-certification-mark.

[3] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0.

[4] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[5] https://www.congress.gov/bill/116th-congress/house-bill/1668.

as well as significant privacy and cybersecurity enforcement[6] by the Federal Trade Commission (FTC) under Section 5 of the FTC Act.

The NPRM poses a multitude of open questions on all aspects of the labeling program – from standards development, compliance assessment, and label structure/components, to enforcement, liability protection, and international harmonization. Further, the NPRM suggests that the Commission is envisioning a potentially complex and onerous regime involving third party product testing and an IoT product registry to be updated in real time.

Together, the complexity of the NPRM and the speed at which the FCC is proposing to move means that a broad range of stakeholders' interests are at stake. Participation by these stakeholders will help ensure that the eventual labeling program provides valuable information to consumers and offers adequate incentives and protections for industry stakeholders to participate.

THE NPRM

The NPRM seeks public comment on numerous issues related to implementation of the cybersecurity labeling program, including:

(i.) The scope of eligible devices or products;

(ii.) Oversight and management;

(iii.) Development of criteria and standards;

(iv.) Program administration;

(v.) Legal authority; and

(vi.) Digital Equity.

Each of these areas is addressed in more detail below.

Notably, while the FCC envisions that it will promulgate regulations to govern the program, and participants will be required to adhere to those regulations, the NPRM does not offer proposed rules.

ELIGIBLE DEVICES OR PRODUCTS

The FCC proposes to initially limit program eligibility to "IoT devices" that "intentionally emit radio frequency (RF) energy."[7] The Commission builds off NIST's definition of "IoT device," defining the term as "(1) an Internet-connected device

[6] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[7] NPRM ¶ 11.

capable of intentionally emitting RF energy that has at least one transducer (sensor or actuator) for interacting directly with the physical world, coupled with (2) at least one network interface (e.g., Wi-Fi, Bluetooth) for interfacing with the digital world."[8] The NPRM does not expressly discuss whether this definition includes phones, but the NIST definition upon which it builds "excludes common general purpose computing equipment (e.g., personal computers, smartphones)."[9]

The Commission seeks comment on the scope of products that are eligible for the program, including:

- Whether the labels should be for an entire product, rather than a device that may be a component within a product.[10]
- Whether the Commission should also include devices/products outside the proposed definition that connect to Wi-Fi via an intermediary (e.g., through a Wi-Fi gateway).[11]
- Whether the program should also include enterprise devices or products for industrial/business use.[12]

The Commission also proposes to exclude from the program any:

(1) Previously authorized equipment that has been identified as "covered equipment" on the FCC's Covered List (i.e., the list of equipment that the Commission has determined poses an unacceptable risk to the United States);

(2) Equipment that, now or in the future, has been placed on the Covered List;

(3) Any IoT device that is produced by an entity identified on the Covered List as producing "covered" equipment; and

(4) Any IoT device that is produced by an entity identified on the Department of Commerce's Entity List, the Department of Defense's List of Chinese Military Companies, or similar lists.[13]

OVERSIGHT AND MANAGEMENT OF THE IOT LABELING PROGRAM

The NPRM envisions a program wherein the Commission – as the "labeling scheme owner" – would be responsible for oversight and management of the program, including

[8] NPRM ¶¶ 11.

[9] NIST, Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products at 3 n.3 (Feb. 4, 2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[10] NPRM ¶¶ 13–14.

[11] NPRM ¶ 15.

[12] NPRM ¶ 16.

[13] NPRM ¶¶ 17–18.

by "creat[ing] and own[ing] a new distinctive trademark to be used in [the program]" and taking "appropriate steps to authorize [the label's] overall use in a way that ensures the integrity of the mark and the label."[14] It further proposes to "leverage the specialized expertise of third parties" by allowing entities to develop requirements or standards for the program and assess other parties' compliance with the program's standards.[15]

To demonstrate compliance with the IoT labeling program, the Commission proposes to create Cybersecurity Labeling Authorization Bodies (CyberLABs), which would be third-party entities with expertise in security and compliance testing and roughly analogous to the Commission's existing Telecommunications Certification Bodies (TCB).[16] The Commission seeks comment on how to structure the application and qualification/accreditation processes for CyberLABs,[17] as well as whether to allow CyberLABs to establish and assess fees for processing accreditation requests.[18]

DEVELOPMENT OF IOT CYBERSECURITY CRITERIA AND STANDARDS

The Commission has not set out exact criteria for compliance beyond a general proposal to use NIST's recommended IoT criteria from that agency's 2022 white paper on cybersecurity labeling.[19] The FCC notes that there are ten NIST criteria:

(1) Asset identification;

(2) Product configuration;

(3) Data protection;

(4) Interface access control;

(5) Software update;

(6) Cybersecurity state awareness;

(7) Documentation;

(8) Information and query reception;

(9) Information dissemination; and

(10) Product education and awareness.[20]

---

[14] NPRM ¶ 21.

[15] Id.

[16] NPRM ¶¶ 24–25.

[17] NPRM ¶ 26.

[18] NPRM ¶ 50.

[19] NPRM ¶ 27. See NIST, Recommended Criteria for Cybersecurity Labeling for Consumer IoT Products (Feb. 4, 2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[20] Id.

The FCC seeks comment on how these criteria could be used to inform minimum IoT security requirements and standards for conformity assessments or for self-attestation.[21] The Commission seeks comment on whether other criteria should be considered and whether higher-risk devices should utilize separate criteria.[22]

The Commission proposes that standards would be developed jointly with industry and other stakeholders.[23] The Commission asks whether the FCC or an outside entity should convene stakeholders to develop standards.[24] The Commission proposes that the process would involve the following steps:

- Collecting information;
- Establishing requirements;
- Developing the standard;
- Reviewing and improving; and
- Implementation.[25]

The Commission seeks comment on additional factors that should be considered in this process, as well as the length of time the process would take to complete.[26] The NPRM also seeks comment on whether the Commission should consider adopting existing IoT security standards, including standards for specific devices or classes of devices.[27]

While participation in the IoT labeling program would be voluntary, the Commission proposes to require participants to adhere to the standards it adopts.[28] Additionally, the NPRM seeks comment on the process for approval of standards including whether the Public Safety and Homeland Security Bureau (PSHSB) should approve standards after notice and comment in lieu of the full Commission.[29]

The Commission seeks comment on the process for conformity assessment. While the NPRM is focused on third-party assessment akin to TCB certification, it also asks whether other procedures, such as the Supplier's Declaration of Conformity (SDoC) in the equipment authorization regime – may also be appropriate.[30]

---

[21] Id.
[22] Id.
[23] NPRM ¶ 28.
[24] Id.
[25] NPRM ¶ 29.
[26] Id.
[27] Id.
[28] NPRM ¶ 30.
[29] NPRM ¶ 31.
[30] NPRM ¶ 32.

ADMINISTRATION OF THE IOT LABELING PROGRAM

The NPRM seeks comment on several issues related to program administration, including the components of the label itself, the creation of an IoT registry, updates to that registry and renewal requirements to allow ongoing use of the label, enforcement of the labeling rules, limitations on liability and preemption for program participants, consumer education, and ensuring international integrity of the label.

IoT Label

The Commission proposes to use a single binary label with layering that will utilize a QR code.[31] Products or devices will either qualify or not qualify for the label, and a scannable QR code will direct consumers to more detailed information.[32] The Commission seeks comment on how to display the label (e.g., affixed to the device or its packaging).[33] Regarding layered information, the NPRM seeks comment on use of a QR code or URL to allow consumers to access information about the device/product, "including specific security information, such as the device manufacturers' level of support, software update history, privacy policy, and similar information."[34] The FCC asks several questions about what the QR code should include, such as whether the QR code will provide information that will not need to be updated or whether the QR code should link to the IoT registry page (discussed in the next paragraph) for the product.[35] The Commission also seeks comment on ensuring the integrity of the label and what features it can provide to improve consumer awareness.[36] Additionally, the FCC seeks comment on how to ensure the accessibility of its label.[37]

IoT Registry

The Commission proposes to create an IoT registry where the public may access information about devices approved under the program.[38] The Commission seeks comment on whether there are similar registries and whether it should select and oversee a third-party registry administrator for the registry.[39] The NPRM asks what information should be included in the IoT registry and how the information should be organized.[40]

---

[31] NPRM ¶ 35.
[32] Id.
[33] NPRM ¶ 36.
[34] NPRM ¶ 37.
[35] NPRM ¶¶ 38–40.
[36] NPRM ¶ 55.
[37] NPRM ¶ 56.
[38] NPRM ¶ 41.
[39] Id.
[40] NPRM ¶¶ 42–43.

Updates and Renewal

The Commission seeks comment on how to keep the relevant security information up to date, noting that cybersecurity risks are constantly changing and require constant updating.[41] The Commission proposes that vulnerabilities and updates be provided through the IoT registry.[42] Notably, the Commission seeks comment on whether manufacturers or importers of the IoT devices and products should be required to "notify the IoT registry operator when they become aware of an unpatched vulnerability that poses security risks to their IoT devices and products."[43] The NPRM also proposes an annual renewal requirement for label applicants.[44]

Enforcement

The NPRM asks several questions about how compliance with the strictures of the labeling program will be enforced, including which agencies or entities should enforce the labeling program requirements, the role of the Commission and other entities in audits and oversight, and whether the Commission should allow consumer or third-party complaints.[45]

Limitations on Liability

The Commission also seeks comment on whether authorization to use the label and compliance with the corresponding security measures may "represent an indicium of reasonableness that might serve as a defense or safe harbor against liability for damages resulting from a cyber incident, e.g., data breach, denial of service, malware."[46] The Commission notes that it does not "intend at this time for the labeling program in and of itself to preempt otherwise existing law."[47]

Consumer Education

The Commission notes that the program will utilize a consumer education campaign.[48] The NPRM seeks comment on whether the campaign should be compromised of recommended NIST materials, and how to fund any outreach campaign, including whether to use "public or private partnerships."[49]

---

[41] NPRM ¶ 45.
[42] Id.
[43] Id.
[44] NPRM ¶ 47.
[45] NPRM ¶ 51.
[46] NPRM ¶ 52.
[47] Id.
[48] NPRM ¶ 53.
[49] NPRM ¶ 54.

International Integrity

Finally, the NPRM seeks comment on how the Commission should "coordinate and engage with other international bodies maintaining labeling programs to develop recognition of the Commission's IoT Label, and where appropriate, mutual recognition of those international labels."[50] It also asks what steps the agency should take to "ensure the FCC label is not mistaken for compliance with IoT security or RF-emission standards in other countries."[51]

LEGAL AUTHORITY TO PROMULGATE THE PROPOSED RULES

The Commission asserts broad legal authority over cybersecurity under Section 302(a)(1) of the Communications Act. Under that provision, the "Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency . . . in sufficient degree to cause harmful interference to radio communications." The Commission reasons that its "proposed labeling program rules are intended to ensure that IoT devices have implemented certain minimum cybersecurity protocols to prevent their being hacked by bad actors who could cause the devices to cause harmful interference."[52]

The Commission also seeks comment on whether it has authority under other provisions of the Communications Act, including:

- Section 302(a)(2), which allows the Commission to promulgate "reasonable regulations . . . establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy."[53]
- Section 333 – which prohibits persons from "willfully or maliciously interfer[ing] with or caus[ing] interference to any radio communications of any station licensed or authorized by or under [the Communications Act] or operated by the United States Government" – in tandem with the FCC's ancillary authority.[54]
- Section 301, which grants the FCC its general licensing authority.[55]

---

[50] NPRM ¶ 55.
[51] Id.
[52] NPRM ¶ 59.
[53] NPRM ¶ 60.
[54] NPRM ¶¶ 60, 64 & n.106.
[55] NPRM ¶ 63.

- Any other source of authority, "including [the Commission's] authority pursuant to Titles II and III as well as its [ancillary] authority."[56]

The Commission also seeks comment on its authority to enforce compliance with the labeling scheme by voluntary participants.[57] In particular, it asks, among other questions, whether "participants in the labeling program [would] already be holders of authorizations within the meaning of section 503(b)(5) of the Act," such that the Commission could enforce the program rules against a participant without first issuing a citation.[58]

DIGITAL EQUITY

Finally, the Commission notes its "continuing effort to advance digital equity for all" and invites comment on equity-related considerations associated with the issues raised by the NPRM and the labeling program.[59]

[56] NPRM ¶ 64.
[57] NPRM ¶ 65.
[58] Id.
[59] NPRM ¶ 66.