



Center for Technology, Innovation and Competition



Penn Law

# RPKI: Legal Barriers and New Directions

Christopher S. Yoo

David A. Wishnick

University of Pennsylvania Law School

February 2019

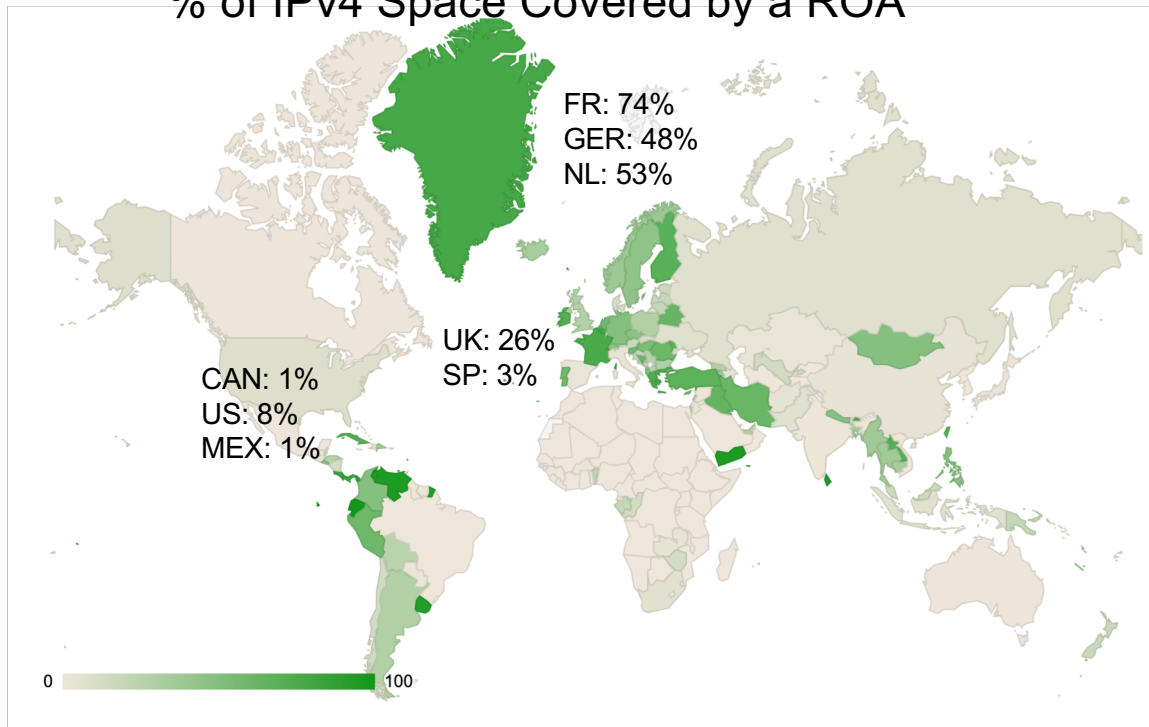
Research supported by NSF EAGER Award #1748362

# 2018: A Big Year for the Resource Public Key Infrastructure (“RPKI”)

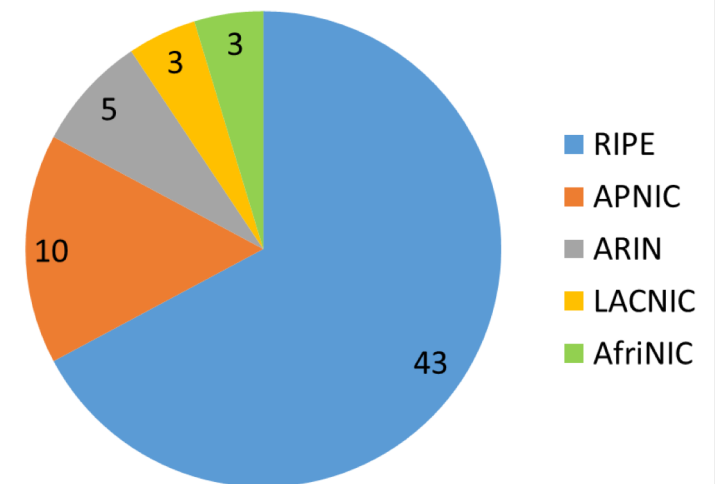
- Cloudflare issued route origin authorizations (“ROAs”) to cover 25% of its prefixes, including its 1.1.1.1 resolver and DNS servers
- NTT now treats ROAs as if they were IRR route(6)-objects
- AT&T/as7018 now dropping all RPKI invalids
- 100+ networks have joined the Mutually Agreed Norms for Routing Security (“MANRS”)
- Google to begin filtering routes in 2019
- The American Registry for Internet Numbers (“ARIN”) allowed integration of its contract into RPKI software workflows and renewed its review of legal issues

# Global RPKI Deployment

% of IPv4 Space Covered by a ROA



Autonomous Systems  
Deploying Route Origin  
Validation (ROV) by Region



- 80% of those engaging in ROV omit the ARIN TAL (Cartwright-Cox, 2018)

# The Legal Aspect of RPKI Adoption

- Legal issues partially explain North America's lag in RPKI adoption
- Research we presented at NANOG 74 aimed to assess the issues
- We refined our preliminary recommendations with the help of the NANOG community
- We released a report and recommendations on December 31, 2018
- 2019: Time to push forward!

# Issue 1: Relying Party Agreement Acceptance

- Leading validator software comes preloaded with all Trust Anchor Locators (“TALs”) except ARIN’s
  - This is because four RIRs allow access without click-through agreements
  - This likely explains some of the disparity in RIR repository utilization
- ARIN requires acceptance of a Relying Party Agreement (“RPA”)
  - American law requires actual or constructive knowledge of the agreement
  - To ensure the terms are binding, they need to be in the user’s visual field

## Reco. 1: ARIN Should Review its RPA

- Two reasonable paths
- ARIN could drop the RPA altogether
  - This would require ARIN to shoulder more legal risk
  - But would enable free redistribution of the ARIN RPKI repository to potential users
- ARIN could keep the RPA, but consider revising/deleting the RPA's indemnification clause
  - The clause creates friction for would-be signers
  - The clause is “belt-and-suspenders” protection—but perhaps not worth it

## Reco. 1: ARIN Should Review its RPA

- Currently, ARIN requires RPs to indemnify for a wide range of risks
- The clause goes well beyond any other RIR

| RIR      | RPA Analogs: Key Clauses Allocating Liability (Paraphrases)   |
|----------|---|
| ARIN     | <ul style="list-style-type: none"><li>• Disclaimers of warranties</li><li>• Indemnify, defend, and hold harmless</li><li>• Applies to claims asserted by third parties in connection with actions taken by the RP or users downstream of the RP</li></ul> |
| AFRINIC  | <ul style="list-style-type: none"><li>• No agreement</li></ul>  |
| APNIC    | <ul style="list-style-type: none"><li>• No agreement; online terms and conditions include indemnification, but no duty to defend or hold harmless</li></ul>   |
| LACNIC   | <ul style="list-style-type: none"><li>• No agreement</li></ul>  |
| RIPE NCC | <ul style="list-style-type: none"><li>• Online terms and conditions include disclaimers of warranties</li></ul>   |


## Reco. 1: ARIN Should Review its RPA

- Originally thought to be the most important legal issue out there
- Our research suggests it may not be a deal-breaker, but is still significant
  - The indemnification clause mirrors what ARIN members sign in their Registration Services Agreements (“RSAs”)
  - But the clause maybe not worth accepting in the RPA context
- We propose an “as-is” disclaimer of warranties as an alternative approach
- ARIN has agreed to consider revising/deleting the indemnification clause
- The community should engage with ARIN to encourage sensible risk-allocation

## Reco. 2: Software Developers Should Consider Integrating the RPA

- Until recently, users had to visit the ARIN website to get the TAL
- In the wake of NANOG 74, ARIN changed its policy

### Software Installation Tools

Software installation tools may download the ARIN TAL on behalf of a user after the user has confirmed their acceptance of the ARIN Relying Party Agreement (RPA) on the ARIN website. This acceptance must require "agreement to the ARIN Relying Party Agreement  (<https://www.arin.net/resources/rpki/rpa.pdf>)" and obtain a non-ambiguous affirmative action by clicking on, or the entry of, a word of agreement (such as "yes" or "accept")

Example:

```
Attention: This package requires the download of the ARIN TAL and
agreement to the ARIN Relying Party Agreement (RPA)
(https://www.arin.net/resources/rpki/rpa.pdf) .
Type "yes" to agree, and you can proceed with the ARIN TAL download: yes
```

- To date, no validator software has integrated the RPA

## Reco. 2: Software Developers Should Consider Integrating the RPA

- The current approach is imperfect in some ways
  - Blocks typical approaches to automated software distribution—RedHat, etc.
  - Requires deviation from open source principles
- Internet engineering has long focused on practicality
  - The ARIN TAL is an important piece of any ROV implementation
  - All sides should explore whether a compromise solution is possible
- Validator software offerings should consider integrating the RPA—potentially a small cost for significant gain vis-à-vis RPKI deployment
- Users should explore enterprise-level agreements (no clickthrough)
- Users should ask paid providers to develop software solutions as well

## Issue 2: The RPA's Prohibited Conduct Clause

- RPA forbids sharing RPKI info in “machine-readable format”
- Clause blocks valuable research and third-party software support
  - Machine-readable analysis is crucial
  - Combined services integrating RPKI with other info (IRR, etc.) is a promising way forward for routing security
- ARIN has agreed to consider revising this clause
- Best process is for the community to engage with ARIN on this issue going forward

## Reco. 3: ARIN Should Forbear from Enforcing Clause Against (Some) Prohibited Conduct

- Third-party security solutions are promising
  - Some solutions combine RPKI data with other information (IRR, analytics) to improve routing security
  - Some solutions use RPKI to clean up IRR data
  - These solutions need to distribute *machine-readable* information that builds on analysis of RPKI info
- ARIN should consider methods that allow approved developers to make use of RPKI information as an input into these more sophisticated services
- ARIN should explicitly allow sharing for research and analysis

## Reco. 4: Community Should Consider Whether to Form a New Nonprofit for RPKI

- The approach described so far: work with ARIN to revise the existing RPA
- An alternate approach: work with ARIN to spin off an entirely new RPKI repository organization
  - Would be the publisher of the North American RPKI repository
  - Would receive verified information from ARIN re repository contents
  - Would require careful legal structuring to ensure ARIN remained functionally separate
  - Would offer a new avenue for managing litigation risk

## Reco. 5: Community Should Consider Whether to Form a New Nonprofit for RPKI

### ■ Potential pros:

- Untethered to existing ARIN operations—might accept more risk
- Could focus its efforts solely on perfecting RPKI implementation

### ■ Potential cons:

- May run up against history
- Might simply arrive at the same conclusions that ARIN reached pre-2018
- Would require a significant collaborative effort to stand up a new organization
  - But many precedents: ARIN, DNS-OARC, PeeringDB are all member-funded



**DNS-OARC**

Domain Name System Operations Analysis and Research Center



**PeeringDB**

## Reco. 6: Law Isn't Everything: Procurement

- To drive the virtuous cycle of RPKI adoption, lowering legal barriers is helpful, but not all-powerful
- *Demand* will be a key driver of success
- We recommend that large purchasers—companies, governments—incorporate RPKI into specifications for supplier
  - ISPs
  - Cloud providers
  - Security services
- Place RPKI on the table not merely as an internal project, but as a request you make of your partners

## Reco. 7: Law Isn't Everything: Best Practices

- RPKI deployment is only valuable if done safely (esp. failover)
- For network operators, there are readymade best practices—and advisers ready to support
  - Operators should follow the advice of the key RFCs—7115, 6480
  - Operators should solicit advice—from MANRS, Internet2, RIRs
- For RIRs, safe deployment requires better clarity and disclosure around service-level intentions
  - Would benefit from dialogue among RIRs
  - Would benefit from expanded Certification Practice Statements
  - May require greater service commitments

## Potential Next Steps

- Software developers should consider building RPA acceptance into their products
- ARIN should consider contract changes
  - Dropping the RPA—or at least altering the allocation of liability
  - Enabling machine-readable redistribution of RPKI info
  - Building a non-member services pathway to private keys
- The North American routing community should consider whether to support the development of a new nonprofit for RPKI publication
- Network operators and RIRs should focus on best practices and high-leverage tactics like requiring RPKI from vendors
- Everyone should keep up the momentum for a virtuous cycle



# Questions and Discussion