University of Pennsylvania Carey Law School

ILE

INSTITUTE FOR LAW AND ECONOMICS

A Joint Research Center of the Law School, the Wharton School,
and the Department of Economics in the School of Arts and Sciences
at the University of Pennsylvania

RESEARCH PAPER NO. 22-31

The Role of Transaction Cost Engineering in Standards Adoption: Evidence from Internet Security

David A. Wishnick
GEORGETOWN UNIVERSITY LAW CENTER

Christopher S. Yoo
UNIVERSITY OF PENNSYLVANIA CAREY LAW SCHOOL

Note to TPRC participants: Thank you for engaging with our paper. This is an early-stage draft. We would value your feedback on any of it. We also note that the paper currently lacks many citations and has not undergone the rigors of a cite-checking process. As a result, we ask that you neither cite nor circulate it.

THE ROLE OF TRANSACTION COST ENGINEERING IN STANDARDS ADOPTION: EVIDENCE FROM INTERNET SECURITY

David A. Wishnick[*] & Christopher S. Yoo[†]

August 2022 draft

Abstract

The growing economic importance of technical standards has heightened the need for a better understanding of why they succeed or fail. While existing literature has scrutinized the role of public governance, particularly in the realms of regulation, antitrust, and intellectual property, to date legal scholars have largely overlooked the role of private organizational and contractual lawyering in determining the path of technical standardization.

In this Article, we explore this dimension through a case study of the effects of private organizational governance and contracting practices on the fortunes of a nascent Internet security standard. The standard, known as Resource Public Key Infrastructure ("RPKI"), is designed to increase the trustworthiness of information about Internet routing. Through analysis of private organizational and contractual documents, semi-structured interviews with participants in the Internet operations industry, and attendance and participation in key industry conferences, we gained an embedded

[*] Associate Professor, Georgetown University Law Center.

[†] John H. Chestnut Professor of Law, Communication, and Computer & Information Science, and Founding Director, Center for Technology, Innovation and Competition, University of Pennsylvania. For helpful comments and conversations, we thank David Hyman, Rebecca Wexler, and participants in the First Annual Cybersecurity Law and Policy Scholars Conference. For the time they took to be interviewed, we thank Steve Bellovin, Jay Borkenhagen, Randy Bush, Dale Carder, kc claffy, John Curran, Andrew Gallo, Yossi Gilad, Greg Hankins, Paul Howell, Olaf Kolkman, Aris Lambrianidis, Martin Levy, Jason Livingood, Carlos Martinez, Doug Montgomery, Sandra Murphy, Karl Newell, Anita Nikolich, John O'Brien, Andrei Robachevsky, Edo Royker, Steve Ryan, Michael Sinatra, Job Snijders, Tony Tauber, Rüdiger Volk, Matthias Wählisch, Russ White, and many others who prefer to remain unnamed. Portions of this Article draw from the authors' report entitled "Lowering Legal Barriers to RPKI Adoption," available at https://ssrn.com/abstract=3308619. The research presented in this Article was supported in part by National Science Foundation Award No. 1748362.

perspective on the role that private lawyering played in shaping would-be adopters' perceptions and decisions regarding the technical standard.

According to our interviewees, contract and organizational bureaucracy mattered greatly. Notably, we found that the terms of contractual agreements prevented some potential adopters from experimenting with the technology and deterred others from proposing that their organizations adopt the technology. This was due to the perceived costs of involving organizational lawyers in technology-adoption decisions. In addition, contract terms deterred actors from increasing the functional value of the standard via complementary innovation and the development of complementary information services. Remarkably, even the basic mechanisms for presenting and assenting to contract terms chilled prospects for adoption. Regarding organization, we found that stark differences of governance and mission between key North American and European nonprofits contributed to different patterns of adoption. Taken together, these findings reveal the continuing importance of old-school transaction-cost engineering even in the most technical realms of Internet operation and standardization.

Table of Contents

INTRODUCTION

What makes a technical standard succeed or fail? From environmental quality (gas vs. electric cars) to the communications environment (Wi-Fi, 5G, HTML…) to ubiquitous computer devices (your screen right now), standards carry unquestioned economic weight. As a result, the determinants of technical standard success have become a core topic of fascination for scholars, policymakers, and private-sector actors alike. Among legal scholars, the study of technical standardization has largely sounded in the fields of intellectual property, where debates over fair, reasonable, and nondiscriminatory ("FRAND") patent licensing looms large, and industrial regulation (including antitrust), where debates center on government agency influence on technical network formation and governance. In each context, legal scholars have tended to focus on how public actors ought to govern the arenas in which technical standardization takes place.

Largely missing from the legal scholarship is the role of private lawyering—what Ronald Gilson famously called "transaction-cost engineering"—in tipping standards adoption pathways in one direction or the other.[1] The transaction-cost engineering ideal holds that lawyers can create value by minimizing the frictions stopping parties from reaching mutually beneficial agreements.[2]

What accounts for this lack? Two hypotheses immediately present themselves. First, private lawyering might simply not matter. Call this the "attorney irrelevance" hypothesis. Though the quality of lawyering may matter a great deal in Gilson's context of corporate transactions, it might not matter much in battles between technical standards. Maybe good technology just always wins out over bad, no matter what the lawyers do.

A second hypothesis has more theoretical origins. For decades, students of digital technologies have suggested—in varying degrees of oracularity—that we have transcended old economic forms and have entered the age of the "network society." Following the sociologist Woody Powell, this form of production, it is thought, engages "neither market nor hierarchy." Instead, it sits outside the realm of legal relations where transaction-cost engineering

[1] Ronald J. Gilson, *Value Creation by Business Lawyers: Legal Skills and Asset Pricing*, 94 YALE L.J. 239, 253-56 (1984). For an excellent survey of the scholarship building on Gilson's insight, see Elizabeth Pollman, *Value Creation by Business Lawyers: Where Are We and Where Are We Going?*, 15 U.C. DAVIS BUS. L.J. 13 (2014).
[2] Gilson*, supra* note 1, at 255.

has import. Gone are the days when *legal* transaction costs determine economic outcomes; only technical frictions matter now.

In this Article, we look to a core site of the network society—Internet security—to shed light on the role of private lawyering in technical standardization. If there is anywhere that good technology should win out over bad, and where lawyerly skill ought not carry weight, it should be the realm of Internet standards—where "kings, presidents, and voting" have given way to "rough consensus and running code."[3] Yet, our study reveals the continuing importance of old-school transaction-cost engineering even in the most technical realms of Internet operation. It turns out that private transactional lawyering matters to the innovation, diffusion, and ongoing operation of core Internet security standards.

The aspect of Internet security we study concerns routing. Routing refers to the path data travel over from one Internet endpoint to another. To identify paths, network operators—such as Internet Service Providers, universities, and governmental organizations—make periodic announcements to each other about the other networks to which they are connected. These routing announcements are usually mundane. Imagine thousands of post offices collaborating on a giant list of different ZIP code adjacencies. But sometimes, negligent or malicious parties publish false routing announcements that prevent users from accessing desired content or divert traffic from its intended destination. These mistaken and malicious announcements impose large costs on Internet users and operators alike.

To make routing more reliable and secure, Internet coordination bodies have encouraged network operators to adopt a technical standard called the Resource Public Key Infrastructure ("RPKI"), which is designed to increase the trustworthiness of routing announcements. RPKI is inexpensive to implement, and it has been available for years. Yet, network operators—to the frustration of many commentators—have been slow to adopt it.[4] Maybe this is because the technology itself is no good. But maybe something else is going on. The fact that RPKI has garnered much better adoption in some regions (Europe and Latin America, in particular) than others (notably North America) suggests the possibility of governance.

---

[3] David Clark, *A Cloudy Crystal Ball – Visions of the Future*, 24 PROC. INTERNET ENG'G TASK FORCE 539, 543 (1992), https://www.ietf.org/proceedings/24.pdf.

[4] *See, e.g.*, Sharon Goldberg, *Why Is It Taking So Long to Secure Internet Routing?*, ACM QUEUE (Sept. 11, 2014), http://queue.acm.org/detail.cfm?id=2668966.

This Article examines the roles of contracting practices and organizational governance in shaping RPKI's uptake. Drawing on the analysis of important agreements that structure RPKI relationships, observation of and participation in Internet security and operations conferences in North America, and a series of semi-structured interviews with a wide range of professionals involved in Internet routing security, we develop a detailed picture of the role of private lawyering in RPKI's adoption trajectory to date.

Our picture suggests that, far from being irrelevant, private contract and organization have been key drivers of network operators' and IP address holders' decisions regarding whether to make use of, or even experiment with, RPKI. Indeed, we find that participants in the Internet security community tend to treat the legal agreements and relationships surrounding RPKI as components of the technical standard itself.

By governing options for use, distribution, and tinkering with RPKI, the legal agreements (and key nonprofit entities that promulgate them) actively shape the way network participants think about the RPKI adoption decision. They affect the intrinsic quality of the RPKI standard: whether it gets improved through innovation. And they affect the level of network externalities that encourage follow-on adoption. By documenting these effects, we demonstrate the ongoing importance of basic private lawyering—contractual and organizational governance—even in the technical standardization of the archetypal digital-age network.

The perspective we develop builds on the "contract as product" metaphor that has been deployed by legal theorists in debates over contractual boilerplate.[5] Call it the idea of "governance components": the attractiveness of a technical standard will often include the quality of the private lawyering and institutional governance that surrounds it. This perspective has implications for scholars and practitioners alike. For scholars, it counsels widening the lens regarding technical standardization beyond patent policy and regulation. It also contributes to literature on the increasing integration of contractual documents and the rest of the technology stack. For practitioners, it suggests the importance of adapting contractual documents to serve avowedly technical purposes, not merely purposes that are traditionally viewed as "legal," such as the reduction of the risk of lawsuits. To the extent network engineers and other developers of technical

[5] *See, e.g.*, Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1126 (2000) (providing a canonical statement of the contract-as-product metaphor).

standards are wary of engaging with the lawyers in their midst, we suggest the value of bridging the two cultures to serve organizational goals.

The Article proceeds in five parts. Part I situates our study within the broader literature on the role of law in technical standardization. Part II describes RPKI as a technology. Part III describes the study's setting and methods. Part IV presents our assessment of the role of contractual governance in the Internet routing security setting. Part V discusses implications beyond contract of institutional actors and the larger community.

I. THE ROLE OF LAW IN TECHNICAL STANDARDIZATION

Technical standards—defined by the Office of Management and Budget as uniform "rules, conditions, guidelines or characteristics" for products, processes, and protocols[6]—surround us. Legal scholarship on contemporary technical standardization has focused mainly on three aspects of the law's role.

The most prominent body of work examines bargaining power in the context of formal standard-development organizations and standard-setting organizations.[7] In particular, it looks to the role of intellectual property rights, patent hold-up dynamics, and reasonable royalty regimes in shaping standardization outcomes.[8] It also has considered questions of antitrust law and policy as they relate to standardization.[9] To the extent this body of work has examined the building blocks of corporate and contractual governance, it has usually been with an eye to their implications for conflicts between small numbers of large firms. By contrast, our study focuses on adoption decisions among a large group of heterogeneous institutions.

A second body of literature concerns the role of administrative agencies in standardization processes. This literature sometimes asks questions of technical substance: whether agencies such as the Federal Communications Commission, Securities and Exchange Commission, or the Department of

[6] OMB Circular No. A-119 Revised, https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf.

[7] *See, e.g.*, JEFFREY H. ROHLFS, BANDWAGON EFFECTS IN HIGH-TECHNOLOGY INDUSTRIES 6, 137-65, 177-78, 201 (2001) (FCC).

[8] *See, e.g.*, Mark A. Lemley & Carl Shapiro, *Patent Holdup and Royalty Stacking*, 85 TEX. L. REV. 1991 (2007).

[9] For leading cases applying antitrust law to standard setting, see, e.g., *Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988); and *Rambus, Inc. v. FTC*, 52 522 F.3d 456 (D.C. Cir. 2008).

Energy ought to promote particular standards in their regulatory domains. It also asks questions about tactics: should the agencies engage in command-and-control regulation or are light-touch approaches? This literature has scrutinized the potential role of regulators in governing path-dependent adoption processes and bolstering (or countering) network effects. Finally, it has also asked whether administrative agencies ought to use their weight as market participants to push standards-adoption efforts forward. To the extent this literature engages with the internal governance of standardization networks, it does so with an eye towards levers for governmental actors to lean on in achieving their ends.

A final body of literature begins works in a theoretical vein, treating technical standards themselves as aspects of the regulatory "net" that governs behavior in social and economic life. From this perspective, technical standardization itself is a kind of lawmaking—or at least a form of governance that operates alongside the lawmaker's power.[10] When this literature has examined the private governance processes that produce technical standards, it has tended to focus on questions of legitimacy.[11]

In this Article, our approach to law and technical standardization is different. Rather than focus on clashes between powerful organizations or questions of legitimacy and policy, we instead turn our attention to more humble matters. Our inquiry looks to the role of that most technical of legal topics: contractual fine print. We ask whether and how fine print matters to the path of technical standardization. Can contract terms associated with a given technical standard affect the innovation process? Can they affect the pace and scope of diffusion? If so, then it will be valuable for scholars and practitioners alike to pay greater attention to private lawyering in the technical standardization context.

II. THE SETTING: INTERNET ROUTING SECURITY AND RPKI

To develop insights into the role of transaction-cost engineering in the technical standardization processes, we present a case study of RPKI, a standard designed to increase the security of Internet routing. This Part introduces RPKI in more context and detail.

---

[10] *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) (famously arguing that "code is law").

[11] *See, e.g.*, Christian Calliess & Ansgar Baumgarten, *Cybersecurity in the EU, The Example of the Financial Sector: A Legal Perspective*, 21 GERMAN L.J. 1149, 1161-62 (2020) (discussing legitimacy in standard setting for cybersecurity).

A. The Problem with the Internet's "Transitive Trust" to Routing

To get from one endpoint to another across the Internet, data packets must be delivered from network to network until they reach their destinations. A given series of hops between networks—say, from UCLA's network to Penn's—constitutes a *route*. *Routing* is the process of selecting the route that a data packet will traverse to reach its destination.

Recently, mistaken and malicious announcements about viable routes between Internet endpoints have imposed significant costs on users, IP address holders, and network operators. For example, the inclusion of erroneous information can lead to *black holes*, in which all attempts to reach a particular location fail, with a famous example being a Pakistan Telecom route announcement that rendered YouTube unreachable for two hours in February 2008.[12] It can also lead to *route hijacks*, which cause requests to be redirected to an erroneous location.[13] For instance, in April 2018, malicious actors redirected traffic meant for Amazon's authoritative Domain Name System ("DNS") service to another location, facilitating theft of $150,000 in cryptocurrency.[14] A similar thirty-minute attack on major credit card processors occurred fourth months later.[15] In June 2019, a significant amount of European mobile traffic was routed through China for two hours.[16] In April 2020, traffic bound for major content delivery networks that support major online platforms, such as Facebook, Google, and Amazon, was redirected through Russia for two hours.[17] The public record of similar

[12] Declan McCullagh, *How Pakistan knocked YouTube offline (and how to make sure it never happens again)*, C|NET (Feb. 25, 2008, 4:28 PM PT), https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/. The global event occurred immediately after the Pakistani telecommunications ministry ordered that YouTube be blocked within Pakistan. *Id.*

[13] Oliver Moll, *Border Gateway Protocol Hijacking*, ANAPAYA BLOG (Nov. 10, 2020), https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions (describing BGP hijacking and cataloging prominent examples).

[14] Doug Madory, *BGP Hijack of Amazon DNS to Steal Cryptocurrency*, ORACLE DEVELOPERS (Apr. 25, 2018), https://medium.com/oracledevs/bgp-hijack-of-amazon-dns-to-steal-crypto-currency-a90dd29cb3ab.

[15] Doug Madory, *BGP/DNS Hijacks Target Payment Systems*, ORACLE BLOGS (Aug. 3, 2018), https://blogs.oracle.com/internetintelligence/bgp-dns-hijacks-target-payment-systems/.

[16] Catalin Cimpanu, *For two hours, a large chunk of European mobile traffic was rerouted through China*, ZDNET (June 7, 2019), https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/

[17] Zak Doffman, *Russia And China "Hijack" Your Internet Traffic: Here's What You Do*, FORBES (Apr. 18, 2020, 7:20 AM), https://www.forbes.com/sites/zakdoffman/2020/04/18/russia-and-china-behind-internet-hijack-risk-heres-how-to-check-youre-now-secure/.

attacks and routing mistakes is growing,[18] and it is reasonable to presume that other incidents have taken place but escaped public notice.

These problems stem from a security weakness in the Internet protocol used to share information about viable routes. That protocol, known as the Border Gateway Protocol ("BGP"), enables networks to advertise to other networks the potential pathways across which they can deliver data to particular endpoints. Individual networks rely on them to determine along which path to forward the data packets they handle.

Despite their foundational role in determining where information is sent on the Internet, BGP announcements do not contain security features to ensure their accuracy. Rather, BGP operates on a "transitive trust" model, where networks often assume that the routes advertised by their neighboring networks are, in fact, viable. This leaves BGP "surprisingly vulnerable to attack."[19]

B. Anchored Trust and the RPKI

Network engineers involved with the Internet's main technical standards-development body (the Internet Engineering Task Force, or "IETF") have designed two complementary frameworks to deal with problems created by BGP's "transitive trust" model. The first, known as path validation, is implemented through BGP Security ("BGPsec"), a protocol suite that provides cryptographic assurance that every AS on an advertised route has authorized its inclusion in that route.[20] For a variety of reasons, many observers have expressed doubts that BGPsec will be fully deployed or be able to deliver on its promises if it is.[21]

The second, known as origin validation, is implemented through RPKI, which cryptographically validates that the last hop of an advertised route is pointing to the AS authorized by the IP address holder to originate the route.[22] RPKI complements BGP's "transitive trust" system with an additional layer of security generated by an "anchored trust" system involving public-key cryptography. RPKI is a two-sided technology that enables (a) IP

---

[18] Tiziano Tofoni, *What is BGP prefix hijacking? (Part 1)*, MANRS (Sept. 8, 2020), https://www.manrs.org/2020/09/what-is-bgp-prefix-hijacking-part-1/ (reporting 14 prefix hijacks per day for the first seven months of 2020).
[19] Goldberg, *supra* note _, at _.
[20] RFC 8205.
[21] *See* Geoff Huston, *A Survey on Securing Inter-Domain Routing Part 2 – Approaches to Securing BGP* (Aug. 3, 2021), https://labs.apnic.net/?p=1467.
[22] RFC 6480.

address holders to publish information regarding authorized routing announcements and (b) network operators to validate routing announcements against that body of published information. This Section discusses the technical structure of that process and some institutional aspects of its operation.

1. RPKI's Two Sides

RPKI's system is based on public-key cryptography. Under RPKI, the five regional Internet registries ("RIRs") responsible for allocating and managing Internet Protocol ("IP") addresses and Autonomous System ("AS") for various regions of the world serve as trust anchors for an authentication system. They do so by allocating private cryptographic keys to the entities to which they issue IP addresses. These keys allow their holders to publish secure digital objects called Route Origin Authorizations ("ROAs"), which establish which ASes are authorized to originate routes associated with particular IP addresses. Address holders can publish their ROAs in the certificate library that each RIR maintains to serve its region. Each RIR stores the location of the certificate library and the public key for accessing those certificates in a file called the Trust Anchor Locator ("TAL").

The existence of these ROAs enables other parties to validate the authenticity of route announcements: One can validate a route announcement by comparing its point of origin with the ROAs contained in the RPKI repository maintained by the RIR that issued the address prefix. This process is known as Route Origin Validation ("ROV"). Networks can then adopt various practices to filter routes based on ROV information, thereby preventing hijackers from rerouting data. The most common form of ROV calls for the network to compare the last AS in the route to reach a particular IP address with the endpoint listed in the ROA certificate cryptographically signed by the holder of that address.

RPKI is only a partial solution to the problem of BGP security because it does not account for the entire routing path. But its value should not be discounted merely because it is not a panacea. As Internet topology shifts toward a world where there are fewer hops between origin and endpoint, a routing announcement's origin represents an increasingly larger proportion of its full path.[23] In the limit, where there is only one hop between origin and endpoint, origin validation is path validation. Thus, the value of RPKI is even higher among parties that utilize short paths to reach each other. Among near

[23] Christopher S. Yoo, *Paul Baran, Network Theory, and the Past, Present, and Future of the Internet*, 17 COLO. TECH. L.J. 161, 180-84 (2019).

neighbors in network topology, RPKI's origin validation framework is a particularly important contribution to routing security.

One important feature of RPKI is its two-sidedness. For RPKI to be successful, there need to be lots of "signers" *and* lots of "validators." The signers are those IP address holders who use their private keys to sign and publish ROAs. The validators are those network operators that filter routes based on the set of publicly available ROAs. The value to validators increases with the number of signers and vice versa. The more up-to-date ROAs there are, the higher the value of engaging in ROV. In turn, the more participants that engage in ROV, the higher the value of issuing ROAs. Roughly speaking, then, the value of adopting either side of RPKI increases with the number of other actors adopting on the other side in the manner of a classic two-sided market.[24]

2. Low Adoption to Date

Despite the fact that leading coordination bodies such as the IETF Working Group on Secure Inter-Domain Routing ("SIDR"), RIRs, and the U.S. National Institute of Standards and Technology ("NIST") have long promoted RPKI adoption,[25] studies indicate that adoption rates remain low globally.[26] On the signing side, the percentage of IPv4 address space covered by ROAs in the region served by the American Registry of Internet Numbers ("ARIN") (covering North American and part of the Caribbean) has lagged behind the levels achieved in the other four RIRs.[27]

---

[24] *See, e.g.*, Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. EUR. ECON. ASS'N 990 (2003) (providing the seminal analysis of two-sided markets).

[25] *See, e.g.*, WILLIAM HAAG ET AL., PROTECTING THE INTEGRITY OF INTERNET ROUTING: BORDER GATEWAY PROTOCOL (BGP) ROUTE ORIGIN Validation (NIST Special Publication 1800-14 2019), *available at* https://csrc.nist.gov/publications/detail/sp/1800-14/final; *Secure Interdomain Routing (sidr): Charter for Working Group*, IETF, https://datatracker.ietf.org/wg/sidr/about/ (last visited September 26, 2021); *Resource Public Key Infrastructure (RPKI)*, RIPE NCC, https://www.ripe.net/manage-ips-and-asns/resource-management/certification (last visited September 26, 2021).

[26] Taejoon Chung et al., *RPKI Is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins*, PROC. ACM INTERNET MEASUREMENT CONF. 2019 (IMC '19) 406, 411 (2019), https://doi.org/10.1145/3355369.3355596 (reporting that between 9.98% and 11.28% of BGP announcements are covered by RPKI as of Dec. 31, 2018).

[27] *Id.* at 409 (reporting the following RPKI coverage levels: RIPE NCC 16.04%, LACNIC 9.33%, APNIC 8.14%, AFRINIC 3.30%, and ARIN 1.47%); Nat'l Inst. of Standards & Tech., *Global RPKI Repository Analysis*, NIST RPKI MONITOR (Mar. 9, 2020) https://web.archive.org/web/20210318002528/https://rpki-monitor.antd.nist.gov/?p=0&s=1

On the filtering side, a recent study indicates that the number of networks engaging in ROV filtering in the ARIN region falls far below the number of networks engaging in ROV filtering in Europe.[28] Another study concluded that 20% of networks engaging in ROV filtering globally do not filter based on the certificate library for the ARIN region.[29]

There are some indications that networks are beginning to show greater interest in RPKI adoption.[30] Leading Internet Exchange Points (IXPs), such as the Amsterdam Exchange, began filtering routes based on RPKI starting in 2017.[31] Major backbone and cloud ISPs, including Amazon, Cloudflare, and Netflix, began filtering in 2020.[32] AT&T, Google, and Comcast have deployed ROV filtering as well.[33] Discussions on the mailing lists and at the meetings of the North American Network Operators Group ("NANOG") and ARIN suggest that others are thinking of joining them soon.

3. Differing Adoption Paths

The design of RPKI contemplates that networks will filter routes based on RPKI information. That is, networks are encouraged to adopt best practices regarding dropping routes that are invalid while also maintaining

[28] *Measuring RPKI Route Origin Validation Deployment*, ROV DEPLOYMENT MONITOR, https://rov.rpki.net/ (last visited Sept. 26, 2021).
[29] Ben Cartwright-Cox, *The State of RPKI: Q4 2018*, BEN'S BLOG (Dec. 20, 2018), https://blog.benjojo.co.uk/post/state-of-rpki-in-2018.
[30] For updates on adopting networks, see *Is BGP safe yet? No*, https://isbgpsafeyet.com/ (posting updates on which networks have adopted RPKI).
[31] *AMS-IX Route Servers*, AMS-IX, https://www.ams-ix.net/ams/documentation/ams-ix-route-servers (last visited Sept. 26, 2021); *RPKI-based origin validation successfully deployed at DE-CIX*, DE-CIX (Mar. 28, 2019), https://www.de-cix.net/en/about-de-cix/news/rpki-based-origin-validation-successfully-deployed-at-de-cix.
[32] Nathalie Trenaman, *Why ISPs must enable RPKI in 2021 for a safer internet*, CAPACITY (Mar. 31, 2021), https://www.capacitymedia.com/articles/3828173/why-isps-must-enable-rpki-in-2021-for-a-safer-internet.
[33] Jay Borkenhagen, *AT&T/as7018 now drops invalid prefixes from peers*, NANOG MAILING LIST (Feb. 11, 2019, 14:53:45 UTC), https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html; Bikash Koley & Royal Hansen, *Expanding our commitment to secure Internet routing*, GOOGLE CLOUD BLOG (Dec. 2, 2020), https://cloud.google.com/blog/products/networking/how-google-is-working-to-improve-internet-routing-security; Jason Livingood, *Improved BGP Routing Security Adds Another Important Layer of Protection to Online Networks*, COMCAST (May 17, 2021), https://corporate.comcast.com/stories/improved-bgp-routing-security-adds-another-layer-of-protection-to-network.

reliable fallback configurations to account for the risk of faults or unavailability of the RPKI service itself.[34]

Networks deploying RPKI can follow different adoption paths. Some networks may filter based on their own ROV analysis. Or, as is often the case with special-purpose additions to Internet security efforts, networks may seek to rely on information provided by third parties that offer ROV either as a commercial or free service. Due to the benefits of specialization and scale economies, the latter might enable growth in the value of RPKI information—for instance, if a private company or open-source provider offered a set of route filters based on RPKI information in tandem with other information, such as information obtained from Internet Routing Registries ("IRRs"), which are databases in which network operators publish their routing policies and routing announcements.[35] Such third-party services may enable small networks to reduce the cost of implementing RPKI by enabling the realization of scale economies or other managerial efficiencies.

In any case, parties conducting ROV need access to the RPKI repositories of the RIRs. From a legal perspective, this means that key issues include (a) access to the RPKI repositories and (b) redistribution of those repositories and information developed based on them.

4. The Role of Trust Anchors

At the root of the whole RPKI system are a handful of organizations that serve as "trust anchors" for RPKI information. These organizations are the five RIRs. In addition to allocating and managing IP addresses and AS numbers held by the Internet's many participating networks around the world, they play two crucial roles in the RPKI framework. First, they allocate the private keys that IP address holders use to sign ROAs. Second, they provide access to repositories containing all the ROAs issued by the IP address holders in their regions, the location of which is stored in their TALs. Because the RIRs have relationships with the IP address holders and network operators in their regions, they can serve as trusted providers of those services to both sides of the RPKI user base.

For North America and parts of the Caribbean—the region on which we focus our study—access to RPKI private keys and the regional RPKI repository is provided by ARIN, which is a private, member-driven, non-

[34] RFC 7115.

[35] *The Internet Routing Registry (IRR)*, APNIC, https://www.apnic.net/manage-ip/apnic-services/routing-registry/ (last visited Sept. 26, 2021).

profit organization. Its budget is in the range of $20 to $30 million annually, which is funded entirely by member registration fees and dues without any governmental support. Founded in 1997, it began participating in RPKI along with its peer RIRs in 2008. The main contracts governing RPKI arise from the relationships between the RIRs and RPKI participants.

III. OUR STUDY

In conducting the research that underpins this case study, we set out to determine whether and how legal barriers were impeding the adoption of RPKI. Over time, we came increasingly (though not exclusively) to focus our research on the role of contract. Contract and contract-related questions that guided our inquiry included: (1) How and why are contractual documents employed to govern RPKI adoption and use? (2) Who designed and implemented RPKI's contractual governance regime, and why? (3) How has contractual governance impacted the reception of RPKI among potential users? (4) Has contract affected the rate of RPKI adoption in different regions?

To gain insight into the causes, mechanisms, and consequences of contractual governance for RPKI, we observed and participated in professional milieus involved in network operations. Our research within these milieus proceeded along multiple tracks, allowing us to gather information from a variety of sources. These included independent analysis of key contractual documents and relevant law and regulation, semi-structured interviews with relevant players in the network operator community, participant observation in and around a variety of network operator and Internet security conferences, dialogue at conferences and on community message boards, and small-group meetings held to discuss RPKI issues among stakeholders.

A. Collection and Analysis of Key Contractual Documents

Our first step in gaining insight into the role of contract in governing the RPKI adoption process was to gather and analyze all the relevant agreements governing the production and use of RPKI information employed by the five RIRs around the world. These agreements largely fall into two buckets: agreements designed to govern the relationship between RIRs and IP address holders interested in issuing ROAs ("authorization-side agreements") and agreements designed to govern the relationship between RIRs and networks seeking access to RPKI repositories for use in route validation and filtering ("validation-side agreements"). These documents

came in a two main formats—textual content visible on RIR webpages and PDF documents available from hyperlinks on RIR webpages.

With documents in hand, we sought to determine which terms had material effects on network operator behavior, whether by shifting incentives or by altering perceptions. In light of community-member interviews, we also increasingly sought to determine whether the formats and methods of presentation of these agreements to would-be RPKI adopters played a role in IP address holder and network operator behavior. In tandem with analysis of the relevant agreements, we conducted research and analysis of background law—statutes, regulations, administrative guidance, and judicial decisions—that might affect the reception and conduct of parties under the relevant contractual documents.

B. Stakeholder Interviews

Concurrently with our legal research and analysis, we conducted interviews with a range of professionals and academics involved in network operations and Internet security work. These interviewees ran the gamut from network engineers to nonprofit leaders to lawyers and computer security researchers. We make no claim regarding the representativeness of our interviewee group of any population; rather, we sought out interviews with field actors who might be in positions to offer relevant perspectives on RPKI and the interaction of RPKI adoption and the law. After identifying an initial set of interviewees based on prior knowledge of a handful of central actors in the RPKI standardization effort, we proceeded to identify new potential interviewees based on the snowball method and by approaching individuals at conferences and other events at various points during our fieldwork.

Our interview method was a semi-structured one. The interviews varied in length from ten minutes to over an hour and a half. We sought to elicit facts and opinions regarding RPKI as a technical matter; the role of law, contractual documents, and legal actors in governing RPKI's prospects for adoption; the institutions and persons whose actions shaped RPKI's development and reception; and potential actions that participants in the field could take to increase the chances of RPKI's success.

C. Participation in Conferences, Message Boards, and Meetings

A third portion of our research involved observation and participation in the network operations and Internet security fields. We attended a range

of events and participated in a range of formal and informal conversations where interested parties gathered to discuss network operations, Internet security, and RPKI specifically. These included meetings of NANOG, Internet2, ARIN, and an informal working group of network engineers interested in debates over RPKI. At some of these meetings, we presented our in-process findings and recommendations to the attendees. At others, we mainly observed. At all of them, we sought out bilateral and small-group dialogue with participants regarding RPKI. In addition, we observed and participated in the NANOG and ARIN online message boards and engaged in email communication with contacts from time to time. These conversations focused on similar topics as our semi-structured interviews, described above.

Throughout our work in the field, our approach was a distinctly non-neutral one; our sample of interviewees and conference conversations was not random, and our stance in the interviews and conversations was to some extent inside the action. Our research goal, however, was to understand in-depth the potential roles played by law, legal documents, and legal actors in shaping RPKI's chances of widespread adoption; not to gain precise statistical measures regarding any given variable. We believe that our footing gave us access we would not otherwise have received into the relevant professional milieus to gain a solid sense of the standard-adoption process as it was happening on the ground.

IV. PRIVATE LEGAL GOVERNANCE THROUGH CONTRACT AS A COMPONENT OF AN INTERNET SECURITY STANDARD

It is common to conceive of technical standards as proprietary or open. The former are typically governed by patents or other protections that place control in the hands of a situationally-powerful firm or consortium pursuing profit. The latter are typically governed by nonprofits, governmental bodies, or unincorporated groups of individual participants in efforts without legally-defined residual economic claimants. RPKI falls in the latter category.

There is a widespread perception that such efforts tend to reject legalism as an operating framework, captured in David Clark's famous dictum, "We reject: kings, presidents, and voting. We believe in: rough consensus and running code,"[36] and in John Perry Barlow's classic techno-utopian *cri de couer*:

> Governments of the Industrial World, . . . I come from Cyberspace, the new home of Mind. . . . You are not welcome

[36] Clark, *supra* note **Error! Bookmark not defined.**, at 543.

> among us. You have no sovereignty where we gather. . . . I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[37]

It is also echoed in the ambitious predictions that open source software and blockchain will obviate the need for law.[38]

Our research provides a counterpoint in that it reveals the importance of contractual governance even in the context of standards designed to promote open adoption and collaboration—where rough technical consensus and running code must arise within the context of legally binding agreements in a manner reminiscent of open source's need to rely on copyright licensing to achieve its goals.[39] The ways in which this plays out—namely, how contractual governance can affect the real and perceived value of a novel standard to its potential adopters—are the subject of this Part.

A. The Decision to Rely on Contract

Once a standard has been developed to the point where it can become operational, one rough measure of its success is the rate at which it is adopted by potential users. From this perspective, RPKI has been something of a disappointment. Adoption rates on both sides of the framework—that is, signing and validation—remain relatively low around the world. They are especially low, however, in North America. Given the importance of network externalities to the attractiveness of a two-sided technical standard like RPKI, early barriers to adoption have the potential to prevent the virtuous cycle that David Evans and Richard Schmalensee have called "network ignition." This Section reports our findings regarding contractual barriers to adoption of RPKI.

---

[37] John Perry Barlow, A Declaration of the Independence of Cyberspace (Feb. 8, 1996), *available at* https://www.eff.org/cyberspace-independence.

[38] *See* Richard Stallman, *Why Software Should Not Have Owners*, *in* FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN 47 (Joshua Gay ed., 2002) (on open source software); PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 193-204 (2018) (on blockchain).

[39] Fabrizio Marrella & Christopher S. Yoo, *Is Open Source Software the New Lex Mercatoria*, 47 VA. J. INT'L L. 807, 810, 825 (2007). Stallman eventually accepted the need to base open source in copyright but continued to resist the use of contract. Richard M. Stallman, *Don't Let "Intellectual Property" Twist Your Ethos*, GNU OPERATING SYS. (June 9, 2006), http://www.gnu.org/philosophy/no-ip-ethos.html.

Decisions about whether to adopt RPKI are made by IP address holders evaluating whether to publish ROAs and by network operators determining whether to engage in ROV. Within those organizations, judgments about RPKI's costs and benefits are most likely to be made by network engineers. As the actors primarily responsible for dealing with the problems RPKI is meant to address, they are the natural advocates for it. Furthermore, these engineers pay attention to the standards-development work that has promoted RPKI. They are often members of professional communities like the IETF, which sets the standards for RPKI, and NANOG, which offers technical support to would-be adopters.

The RPKI adoption decision involves considerations beyond the technology's merits. Network engineers face myriad demands on their scarce time and financial resources. As a result, they must weigh the value of adopting RPKI against its costs—including the opportunity costs of foregone effort on other projects. They must also consider whether other departments and functions within their organizations have stakes in the decision to adopt RPKI, which varies by organization based on their particular risk and legal review practices.

This is one place where legal questions come into play. Because RPKI raises potential operational risks if not implemented properly, network engineers interested in adopting it must consider whether and how to engage their colleagues in legal and procurement departments. They must weigh the cost of such engagement both in terms of time and institutional capital. Budgets are not infinite, and RPKI is a technically complex framework to explain. As a result, any issue—even a seemingly small one—can introduce transaction costs that put a weight on the scale against adoption, especially during the early stages of the accumulation of network effects, where the value of adoption to first movers can be low. This is not unique to RPKI, of course, but it can be significant.

Perhaps the most distinctive feature of ARIN's RPKI implementation is the requirement that every actor seeking to access the TAL download it individually from its website rather than allowing software to be distributed with its TAL preloaded. The reason is to have every actor relying on its RPKI services agree to a contract known as the Relying Party Agreement ("RPA").

When distributing an RPKI repository, should an RIR require a relying party to enter into an agreement at all? This was a central question raised by many interviewees. Interviewees noted that three of the five RIRs enable access to their RPKI repositories without placing them behind an explicit relying party agreement like ARIN's RPA. Similar security regimes do not

require an agreement similar to the RPA. For example, the Internet Assigned Numbers Authority ("IANA") does not require an RPA for its DNS Root Zone Trust Anchors. Relying parties are unlikely to be bound by anything like an RPA in the TLS context. ARIN itself does not require an RPA for parties that utilize its IRR information. Interviewees suggested that the value of North American ROAs would vastly improve if ARIN opted for a similar agreement-free path in the RPKI context. This is because parties worldwide would have an easier, less legalistic path to conducting ROV on routes covered by those ROAs. In turn, this would increase the value of route-signing in North America.

In deciding how best to structure legal limitations on access to the ARIN Repository, it is necessary to frame the proper goal. ARIN's mission as a "nonprofit member-based organization that supports the operation and growth of the Internet"[40] suggests that one sensible goal for the Internet community, as discussed above, is widespread distribution of RPKI repository information. If this were the only consideration, foregoing contract altogether would help the friction impeding the adoption of RPKI.

Another goal, of course, is to ensure the ongoing stability and soundness of ARIN—a crucial organization in North America's Internet governance. Operating an RPKI repository could create liability under tort law, most likely under a theory of negligent misrepresentation.[41] Questions about particular breaches of duty and the vagaries of causation often generate knotty questions of fact, particularly when it comes to highly technical matters. Furthermore, even defending against claims that ultimately prove unsuccessful can still be costly—especially when questions of fact are involved. The greater litigiousness of American society also makes this risk more important to manage in the U.S. than in other regions of the world. The RPA protects ARIN from undue liability, so any proposal to change it or eliminate it should be approached with caution.

Plainly, these two goals are sometimes in tension. Though some RPKI advocates would wish for RPKI information to flow completely freely, the wisdom of that approach cannot be assumed *a priori*. RIRs have important interests—in proper repository use and appropriate allocation of liability for misuse, for example—that reasonably inform how they offer their TALs to potential users.

---

[40] *About*, ARIN, https://www.arin.net/about/ (last visited Sept. 26, 2021).
[41] Christopher S. Yoo & David A. Wishnick, *Lowering Legal Barriers to RPKI Adoption* 17-21 (Univ. of Pa. CTIC Report Dec. 31, 2018), *available at* https://ssrn.com/abstract=3308619.

By the same token, for an RIR interested in supporting RPKI adoption, complete insulation from potential legal risks is not a feasible goal. Any organization that takes productive action in society cannot completely eliminate the risk of liability or of having to defend against lawsuits—even frivolous ones over entirely legitimate conduct. Instead, the proper objective for an RIR is to balance the risks of incurring legal costs against the benefits of engaging in activities that further the organization's goals. This means that legal protection is an exercise in optimization and appropriate allocation of risk, not necessarily maximization of legal protections.

A proper assessment of how to strike the appropriate balance depends on comparing the best-case scenarios that minimize the exposure to tort liability in the absence of a contract on the one hand and that minimize the transaction costs in the presence of a contract on the other. When it comes to distribution of RPKI repositories, striking the proper balance between potential benefits and risks must take place amid conditions of uncertainty. RPKI is a new service, and we know of no lawsuits dealing with the proper apportionment of the potential sources of liability associated with it. Furthermore, the exact harm scenarios will shift both with increased deployment and as new uses for RPKI information develop. Each RIR and relying party must therefore evaluate its legal risk based on its own best assessment of how RPKI usage might go wrong and where their liability might lie and weigh those risks against the potential benefits of broader RPKI deployment. RIRs and relying parties can gain additional perspective into potential liability from RPKI failure by drawing comparisons to other situations where providers of similar types of trusted information have been subject to legal claims.

At its root, an RPKI repository is a body of information. It holds information necessary to conduct ROV, including Resource Certificates, Certificate Revocation Lists, and signed objects (including, most importantly, ROAs). Though RIRs currently publish the leading RPKI repositories, they are not the creators of the information contained within them. To the contrary, much of the most important information—specifically, the ROAs pertaining to specific locations—can be produced only by the parties that hold private keys pertaining to specific IP address space.

Providers of information might face claims under a few different legal theories. In the case of RPKI, scenarios giving rise to a legal claim include incidents that make it impossible or difficult for traffic to reach an Internet endpoint and incidents that allow traffic to pass into unwanted hands. How might a repository provider like ARIN be implicated in such incidents? Given RPKI's limited track record, it is impossible to be certain, but we conjecture

that an aggrieved party might accuse ARIN of failing to issue private keys to IP address holders in a proper manner, facilitating the issuance of faulty ROAs (whether through administrative error or security failure), failing to provide adequate support for certificate libraries to ensure sufficient up time, or improperly revoking private keys or ROAs. Aggrieved parties might include network operators, IP address holders, and downstream customers whose traffic has been disrupted or misdirected.

One obvious scenario worth considering is how downstream users of RPKI information might react if an RIR's certificate repository were to become temporarily unavailable. This is not fanciful: RIRs' repositories have gone down in the past, including outages for RIPE NCC's RPKI repository in 2013[42] and for ARIN's RPKI repository in 2018 and 2020,[43] and no amount of diligence can eliminate the possibility of similar temporary outages in the future. Indeed, even a resource guaranteed to be available 99.999% of the time may be down a little more than five minutes a year.

To date, these events have had little impact on Internet traffic.[44] That may be because networks that utilize ROV find it easy and sensible to adopt best practices that respond gracefully to outages and similar problems, such as by failing open or by relying on the last validated route. But it also may be because RPKI is in such early stages of deployment. If some networks are unprepared to handle the occasional outage—a possibility that can never be completely precluded—then misconfigurations could, under certain circumstances, lead to traffic disruptions once RPKI ROV is in widespread use. In such a situation, an RIR might be accused of contributing to the misfortune despite the requirement for relying parties to utilize best practices in their use of RPKI information. For this and similar reasons, agreements with users of RPKI are attractive to RIRs.

---

[42] *RIPE NCC RPKI Repository Outage*, RIPE NCC (Feb. 3, 2013), https://www.ripe.net/support/service-announcements/service-announcements/ripe-ncc-rpki-repository-outage. Réseaux IP Européens Network Coordination Centre ("RIPE NCC") is the RIR serving Europe and Western and Central Asia.

[43] Mark Kosters, *ARIN RPKI Repository (Update)*, ARIN (Oct. 24, 2018), https://www.arin.net/vault/announcements/2018/20181024_update.html; Mark Kosters, *12-13 August RPKI Outage: Update*, ARIN (Aug. 26, 2020), https://www.arin.net/announcements/20200826/.

[44] Nimrod Levy, AT&T, Dropping RPKI invalid routes in a service provider network, Lightning Talk: at NANOG 75 (Feb. 19, 2019), available at https://www.youtube.com/watch?v=DkUZvlj1wCk (discussing AT&T's experience deploying RPKI).

B. The Reliance on Browsewrap as the Mechanism for Registering Assent

Turning first to how to minimize the transaction costs of relying on contract, a critical question is what actions are required to signal sufficient assent to the contract to obtain access to the TAL. ARIN had initially structured the agreement as "clickwrap"—a term for legal agreements that require affirmative assent via a mouse-click. NANOG participants raised objections as early as 2014 that requiring clickwrap acceptance to access the TAL was impeding RPKI deployment.

In response to these concerns, ARIN reviewed its approach to offering the RPKI repository to third parties and decided in February 2016 to restructure the agreement into a "browsewrap" agreement by prominently displaying on the website for accessing the TAL the statement that "use of the resources constitutes an agreement to be bound by the terms contained in the document accessible through a link on the webpage" adjacent to a link to the RPA and by treating any subsequent use of the TAL as assent to the RPA.[45] Though courts are wary of enforcing browsewrap against unwitting parties, they are willing to do so where parties have actual or constructive knowledge of the agreement's existence.[46] This is especially true if the party is sophisticated.[47] As a result, ARIN's RPA would likely be held to bind network operators utilizing ARIN's RPKI repository. This change obviated the need for end users to make an affirmative mouse-click explicitly accepting the terms and conditions contained in the RPA before accessing ARIN's repository. According to multiple interviewees, this change resulted in increased willingness among some network engineers to make use of ARIN's repository, as entering into browsewrap agreements falls within their understanding of their authority to act unilaterally within their organizations.

---

[45] This means that the webpage visitor does not need to affirmatively click on an acceptance box in order to access resources, but the webpage states that use of the resources constitutes an agreement to be bound by the terms contained in the document accessible through a link on the webpage. That statement and the link are prominently displayed in a visitor's visual field. Though courts are wary of enforcing browsewrap against unwitting parties, they are willing to do so where parties have actual or constructive knowledge of the agreement's existence. This is especially true if the party is sophisticated. As a result, ARIN's RPA would likely be held to bind network operators utilizing ARIN's RPKI repository.

[46] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 402 (2d Cir. 2004) (holding that actual knowledge of a browsewrap agreement sufficed to establish assent).

[47] Woodrow Hartzog, *The New Price to Play: Are Passive Online Media Users Bound by Terms of Use?*, 15 COMM. L. & POL'Y 405, 417, 419-23, 429-30 (2010); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 463-64 (2006).

The shift to browsewrap as the mechanism for registering assent did not completely satisfy the community. A number of interviewees noted that, unlike the other four RIRs, who permitted the preloading of their TALs in third-party software packages without having to accept any RIR terms of service. ARIN's requirement of affirmative browsewrap assent prevents the inclusion of its TAL in the same manner, as does the provision of the prohibited conduct clause prohibiting sharing the TAL with third parties.[48] That means RPKI validator software, such as the popular package provided by RIPE NCC, comes with only four of the five RPKI repositories preloaded and a page stating that "[t]o access ARIN's [resources], you will have to agree to ARIN's Relying Party Agreement. Please visit [ARIN's] web page for more information." Similarly, a validator provided by Dragon Research Labs included access to four of the RIRs' repositories but omitted ARIN's.

The requirement of agreeing to the RPA to gain access to ARIN's repository raised technical and institutional concerns for interviewees. As a technical matter, interviewees reported that ARIN's browsewrap barrier made the technical task of route-origin validation more onerous. In particular, it inhibited a labor-saving mechanism built into the most popular third-party validation software packages. This raised the risk that engineers would forget or refuse to download ARIN's repository resources or simply abandon the effort to engage in validation altogether. While, given time and focus, the process of downloading and incorporating the ARIN repository into validation software is well within the capacity of the average network engineer, time and focus are inevitably in scarce supply. Especially because mistakes in the configuration of RPKI validation software can have negative consequences, network engineers are loath to implement ROV into production unless they are confident it can be managed effectively over the long term.

Over the course of our research, we had the opportunity to see how legal and technical concerns over the browsewrap barrier were negotiated and reformed. Specifically, network engineers presented their concerns over the browsewrap barrier to ARIN leaders in multiple fora. As a result of that dialogue, ARIN leaders consulted their lawyers and decided to enable third-party software providers to collect assent to the RPA as a part of their user interfaces, rather than requiring separate visits to the ARIN website.[49] This facilitation of turnkey ROV solutions was an act of legal transaction-cost

[48] ARIN RPA, *supra* note _, § 5.

[49] John Curran, President and CEO, ARIN, Software installation tools retrieving ARIN TAL (was: Re: ARIN RPKI TAL deployment issues), NANOG MAILING LIST (Oct. 13, 2018, 13:35:36 UTC), https://mailman.nanog.org/pipermail/nanog/2018-October/097528.html.

engineering that enabled a form of technical engineering that had previously been impossible.

Taken together, these two moments show that even the basic mechanisms of securing assent to an agreement can affect the technical standard-adoption process. In situations where software automation is likely to be valuable from a technical perspective, lawyers and their clients ought to pay attention to the technology of contractual assent.

C. The Potential Chilling Effect of Certain Contract Terms

In addition to technical concerns, many interviewees claimed that the inclusion of particular contract terms in the RPA caused institutional friction sufficient to delay or prevent RPKI adoption: specifically, an indemnification clause, a choice of law clause specifying that disputes would be resolved under Virginia law, and an arbitration clause. Network engineers within some organizations stated that they were wary of entering into the RPA out of fear of running afoul of their organizations' procurement rules. This finding highlights the importance of understanding the organizational sociology at work in technical standards-adoption decisions.

Of these clauses, the indemnification clause raised the greatest concerns. In particular, interviewees stated that their institutional procurement policies prohibit employees from entering into agreements that contain indemnification clauses and other terms not seen in standard licenses without first subjecting those agreements to internal review. These internal review processes require network engineers to invest time in navigating corporate bureaucracy to try out things like RPKI. Internal bureaucracy can be valuable to ensuring that all parts of an organization (for instance, engineering and legal) are on the same page about a new endeavor and any related risks that arise from new dependencies on external services, but they also make new endeavors more time-consuming to undertake.

Some network engineers further stated that the indemnification clause in ARIN's RPA exceeds what their organizations would be willing to accept to participate in ROV. Our interviews with legal personnel suggested a more moderate position: that indemnification is not typically an automatic deal-breaker, but rather acts as a weight on the scale. Regardless, the RPA's indemnification clause clearly posed a nontrivial barrier to experimentation and adoption of RPKI.

In addition to the general issues surrounding direct access to the ARIN RPKI repository, interviewees also raised issues specifically applicable to

government entities. These have to do with terms in the RPA that government agencies regard as problematic. First, federal procurement law prohibits federal actors from authoritatively agreeing to the RPA's indemnification clause.[50] Second, under some circumstances, federal agencies are discouraged from agreeing to alternative dispute resolution procedures like arbitration.[51] Third, similar prohibitions operate at the state and local level and also sometimes forbid accepting agreements that specify the choice of law outside the state in which the governmental entity sits.[52]

This set of barriers for governmental actors required further legal work to resolve. Specifically, ARIN adopted a policy of modifying both clauses for governmental entities to the extent necessary to comply with applicable law or regulations.[53] In theory, this policy eliminated the concerns raised by interviewees about governmental entity access; though how well-known it was we did not ascertain.

For private actors and governmental actors not subject to legal restrictions on their ability to agree to indemnification clauses, the question remains: What does the indemnification clause do? Is it just a wasteful barrier to adoption, or does it serve some valuable transactional purpose?

---

[50] The Anti-Deficiency Act prohibits government employees from authoritatively agreeing on behalf of the government to "unrestricted, open-ended indemnification agreement[s]" like the one in ARIN's RPA. *See* The Anti-Deficiency Act Implications of Consent by Government Employees to Online Terms of Service Agreements Containing Open-Ended Indemnification Clauses, 36 Op. O.L.C. at 1, 2012 WL 5885535 (Mar. 27, 2012), *available at* https://www.justice.gov/file/20596/download ("A government employee with actual authority to contract on behalf of the United States violates the Anti-Deficiency Act by entering into an unrestricted, open-ended indemnification agreement on behalf of the government. A government employee who lacks authority to contract on behalf of the United States does not violate the Anti-Deficiency Act by consenting to an agreement, including an agreement containing an unrestricted, open-ended indemnification clause, because no binding obligation on the government was incurred.").

[51] *See* 5 U.S.C. § 572(b).

[52] *See, e.g.*, 1 CAL. STATE CONTRACTING MANUAL § 7.86 (2017), *available at* http://www.dgs.ca.gov/Portals/32/Users/141/25/3725/8%20Pages%20from%20SCM%20June%202017-3.pdf (prohibiting agreement to indemnification clauses); Katherine A. Adams, Contract Law for State Purchasing Officers § III.G (Sept. 23, 2013), *available at* https://www.naepnet.org/resource/collection/A9EC9928-E0AA-4604-85AE-28941F4BE73C/Contracting_101_Handbook.docx (discussing rules governing choice of law clauses for Kentucky government entities).

[53] *See Registration Services Agreement (RSA) FAQ*, ARIN, https://www.arin.net/resources/agreements/rsa_faq.html (last visited Dec. 27, 2018) [hereinafter "ARIN RSA FAQ"].

At its root, indemnification requires the relying party to bear the burden of various costs associated with a covered set of legal risks. In case of the RPA, the covered set of legal risks is expansive. The RPA's indemnification clause covers "any and all claims" that are "asserted by a third party in connection with" two types of events—(i) the use of RPKI information and services or (ii) the breach of the RPA's terms.[54] The clause covers situations where the use or breach was by the relying party or by any "[a]ssociated [p]ersons," such as customers or clients.[55]

ARIN's indemnification agreement is quite protective of the organization's interests. The key terms—"indemnify, defend, and hold harmless"—impose distinct responsibilities.[56] First, the duty to "indemnify" would require the relying party to pay for a covered set of losses suffered by ARIN after they were established through a legal process. Separately, the "duty to defend" would require the relying party to cover the ARIN's "expense of defending suits" alleging harm from covered activities.[57] Finally, some courts would treat the obligation to "hold harmless" as a right of ARIN to be released from suit brought by the relying party. Restated, the clause insulates ARIN from the monetary costs of adverse legal outcomes. And even before such an outcome might come to fruition, the "duty to defend" would require a relying party to cover the costs of legal defense of all claims falling within its scope. This right to defense would be available to ARIN early in litigation—before a court reached the merits of an underlying suit. As a result, it would allow ARIN to avoid litigation costs associated with even meritless claims brought against it.

At the same time, some interviewees regarded the RPA's indemnification clause as a barrier to RPKI adoption. This is due in part to its mere existence and due in part to its particular terms. Recall that many organizations require formalized review of any agreement containing an indemnification clause. This costs time and deters network engineers from proposing RPKI within their organizations.

---

[54] Specifically, "any and all claims, demands, disputes, actions, suits, proceedings, judgments, damages, injuries, losses, expenses, costs and fees (including reasonable attorneys' fees and expenses), interest, fines and penalties of whatever nature." ARIN, Standard Relying Party Agreement § 7, https://www.arin.net/resources/manage/rpki/rpa.pdf (last visited Sept. 26, 2021) [hereinafter ARIN RPA].

[55] *Id.*

[56] *Id.*

[57] *Capital Envt'l Servs., Inc. v. N. River Ins. Co.*, 536 F. Supp. 2d 633, 640 (E.D. Va. 2008) (applying Virginia law) (internal quotation marks omitted).

The clause's terms are also more stringent than some organizations would likely accept for the purpose of participating in RPKI as early adopters. In particular, the clause is quite broad: it requires relying parties to indemnify ARIN even for its own negligence. Insulating ARIN from liability for conduct problems within its control creates a problem of moral hazard. ARIN is the best-positioned party to reduce the risks caused by its own negligence and thus should certainly bear that burden. Further, ARIN is well-positioned to reduce the ultimate risk of harm through investments in the quality of its provision and through clear disclaimers applicable to relying parties. In October 2019, ARIN partially addressed these concerns by revising the indemnification clause to exclude claims "aris[ing] from ARIN's gross negligence or willful misconduct."[58] This piece of transaction-cost engineering was designed to reduce, though not eliminate, the risk of moral hazard: even the revised clause continues to insulate ARIN from liability for its own negligent conduct that does not rise to the level of gross negligence.

To the Internet routing community, the indemnification clause posed a clear tradeoff between the legal risk-reduction benefits it created for ARIN and the drag it imposed on RPKI adoption.[59] Though we cannot say definitively, there are reasons to think that ARIN overweighted its own self-preservation in deciding to maintain a fairly strict indemnification clause. Though the elimination of the indemnification clause would shift some legal costs from relying parties to ARIN at the margin and may drive up ARIN's insurance costs, the shift would simultaneously remove a clear barrier to RPKI adoption. Notably, as noted earlier, ARIN *already* makes this tradeoff in some cases: it willingly drops the indemnification clause for certain governmental counterparties.[60] This suggests that the clause may not be strictly necessary.

Furthermore, the risk-reduction function of the indemnification clause is only relevant to the extent ARIN is likely to face legal risk for incidents involving RPKI. Though this risk is difficult to estimate, two factors suggest it is not grave. First, the RPA also includes a disclaimer of warranties and

---

[58] ARIN RPA, *supra* note 54, § 7; *accord* John Curran, *ARIN Announces New Relying Party Agreement (RPA) To Spur Use of RPKI*, ARIN (Oct. 21, 2019), https://www.arin.net/vault/announcements/2019/20191021.html.

[59] Interviewees noted that they were wary of binding their organizations to defend and indemnify ARIN for such a broad swath of activity. Further, they stated they were wary of indemnifying ARIN when the value of RPKI is unclear and when they were unsure of ARIN's investments to ensure that RPKI functions reliably on a day-to-day basis. These factors have deterred a number of potential adoptees from advancing RPKI within their organizations.

[60] *See supra* note _ and accompanying text.

liability.[61] This provision can mitigate much of the legal risk posed by RPKI. That is because contract clauses that explicitly limit liability and establish that the agreeing party assumes various risks often suffice to defeat negligence claims (and similar claims of breach of implied warranties) asserted by parties to the agreement. For instance, in Virginia, the jurisdiction whose law the RPA selects to govern disputes, courts have admitted contract clauses as evidence of the express assumption of risk by a party participating in a risky activity. Virginia courts also honor clauses limiting liability in some circumstances. Finally, Virginia law tends to allow parties to disclaim liability for a counterparty's consequential damages in transactions like the RIR-relying party transaction. It is reasonably likely that courts would uphold similar clauses found in the RPA. Such clauses—analogous to the "as-is" license language that typically accompanies open-source software—enable a service provider to bind direct counterparties to a contractual allocation of risks and would provide substantial (though certainly not total) protection against liability. It would also bring ARIN in line with the approach taken by RIPE NCC, which also disclaims liability.[62]

Second, ARIN's choice to impose an indemnification clause is also more burdensome than approaches taken by IANA with regard to its DNS Root Trust Anchors,[63] the providers of the OpenSSL Toolkit,[64] or ARIN's approach to its Internet Routing Registry.[65] Our research has not revealed negligence suits involving trust anchors for comparable security information. This absence is suggestive, but it is not dispositive. If a widespread RPKI outage were to harm many customers of ARIN's relying parties, then the indemnification clause would indeed protect it from serious legal risk. Further, other security resources are provided against the backdrop of indemnification clauses, as are many Internet services—including residential "last mile" service.[66] The Terms of Use for ARIN's Whois Terms of Use,

---

[61] ARIN RPA, *supra* note 54, § 6.

[62] *See RIPE NCC Certification Repository Terms and Conditions*, *supra* note _, art. 4. AfriNIC and LACNIC, for their parts, appear not to have comparable disclaimers of liability at all, let alone indemnification agreements.

[63] *See Trust Anchors and Keys*, IANA, *available at* https://www.iana.org/dnssec/files (last visited Dec. 27, 2018).

[64] *See License*, OPENSSL CRYPTOGRAPHY AND SSL/TLS TOOLKIT, *available at* https://www.openssl.org/source/license.html (last visited Sept. 26, 2021).

[65] *See* ARIN IRR, *supra* note __.

[66] *See, e.g.*, digicert, Certificate Services Agreement §§ 6.3-6.4 (Apr. 12, 2017), *available at* https://www.digicert.com/wp-content/uploads/2017/06/Certificate-Services-Agreement.pdf (indemnification limited to claims arising out of the actions of the customer or customer's agent); Comcast Cable Commc'ns, LLC, *Comcast Agreement for Residential Services*, XFINITY,

which network operators likely encounter through their typical operations, also contain an indemnification clause to which (at least to our knowledge) network operators have not objected.[67] Similarly, providers of DNS services require their users to indemnify them.[68] But all this is merely suggestive. The real question is one of optimization. Given the costs of the indemnification clause on ROV adoption and ARIN's ability to insulate itself from a significant bulk of liability risk through the use of disclaimers and explicit statements of risks, there are good reasons to think a strong indemnification clause went too far.

Our findings on this point suggest that non-standard terms—if noticed by nonlawyers—may be enough to chill those nonlawyers from seeking involvement with a contractually governed technology.

D. The Impact of the Prohibited Conduct Clause on Research and Innovation

A different provision of ARIN's RPA known as the "prohibited conduct clause" also hindered the deployment of RPKI not by impeding its adoption but rather by deterring community members from taking an active role in developing best practices and learning-by-doing with RPKI. Through at least February 2019, this clause stated that information derived from the ARIN Repository may be made available to third parties only "so long as such use and disclosure is solely for informational purposes, namely reporting, educational, summary or statistical purposes, and such use and disclosure of the information *is not in a readily machine-readable format*."[69]

A number of interviewees raised the concern that the prohibition on distributing any RPKI-derived information in "machine-readable format" was inhibiting the deployment of RPKI. One interviewee described potential research on various aspects of RPKI implementation designed to support best-practice development. Others described the potential for analysis of

---

https://www.xfinity.com/Corporate/Customers/Policies/SubscriberAgreement (last visited Sept. 26, 2018); Charter Commc'ns, Inc., *Charter Residential Internet Service Agreement*, SPECTRUM, https://www.spectrum.com/policies/residential-internet-tc.html (last visited Sept. 26, 2018).

[67] *See, e.g.*, *Whois Terms of Use*, ARIN § B.5 (Apr. 9, 2014), https://www.arin.net/whois_tou.html.

[68] *See, e.g.*, *Oracle Services Agreement*, ORACLE DYN § 14 (Apr. 6, 2017), https://dyn.com/legal/dyn-services-agreement/.

[69] American Registry for Internet Numbers, Ltd., Resource Certification Relying Party Agreement § 5_ (version available on Feb. 28, 2019) (emphasis added), *available at* https://web.archive.org/web/20190228033440/https://www.arin.net/resources/rpki/rpa.pdf.

RPKI repositories in conjunction with other data sources to produce higher-value information with which to conduct route-filtering.

The costs of this clause came in the form of limits on complementary innovation and know-how. Network operators routinely share operational information to learn from each other's experiences and to coordinate responses to cybersecurity.[70] Crucially, such information is far more valuable when in machine-readable format because it enables sophisticated analysis and trendspotting.

In another example of useful transaction cost engineering, ARIN announced in October 2019 that it was changing the RPA to allow the distribution of data derived from RPKI for informational purposes in machine-readable formats.[71] This change removed one source of friction inhibiting standard industry practices essential to promoting RPKI's effectiveness.

The change to the prohibited conduct clause only went so far, however. It authorized broader sharing of RPKI-derived data for informational purposes while continuing to forbid such sharing for operational purposes, particularly network routing.[72]

The provision of the prohibited conduct clause barring the sharing of RPKI-derived data for operational purposes is intended to protect ARIN against liability for accidents involving certain uses of its repository information. Consider the following hypothetical situation. Imagine that a party relying directly on information obtained from ARIN's RPKI repository simply redistributed that information free of any agreement to anyone who asked for it. This could potentially open up ARIN to exactly the kinds of tort claims against which the RPA is designed to protect. The prohibited conduct clause defends against this hypothetical by placing the onus on relying parties to ensure that all users using information that they download from the ARIN RPKI repository are bound by the RPA.

Multiple interviewees stated that the prohibited conduct clause is an impediment to important software- and service-development efforts for

[70] *See, e.g.*, *Information Sharing and Awareness*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Sept. 14, 2021), https://www.cisa.gov/information-sharing-and-awareness ("Information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation.").
[71] Curran, *supra* note 58; *accord* ARIN RPA, *supra* note 54, § 5 (omitting the prohibition on distribution in machine-readable formats).
[72] ARIN RPA, *supra* note 54, § 5.

RPKI. Network operators may look to implement RPKI through third-party vendors, as is currently common with DNS. These third-party vendors may wish to incorporate RPKI into comprehensive packages of cybersecurity services.

In addition, cybersecurity providers are beginning to use RPKI in ways that fall outside of its intended use. For instance, services are emerging that use RPKI origin validation to clean up the information contained in their IRRs. Others combine RPKI information, IRR information, and other inputs to create dynamic route-filtering advice for end users. End users employing these emerging services do not necessarily need to access the RIR RPKI repositories directly to benefit from RPKI. The same is true with services that translate RPKI ROAs into IRR objects and with public monitoring projects, such as Certificate Transparency reporting.

There are ways of lawyering around these problems. Our initial report recommended that ARIN consider allowing distribution of services making use of RPKI information as an input on the condition that they require users to accept the RPA or an appropriate variant of it for the use case involved.[73] This would be quite similar to the allowance ARIN has made for designers of validation software, but it would extend to more robust service providers. Alternatively, we recommended that ARIN could require these robust service providers to protect ARIN via an intended third-party beneficiary clause.[74] This is a common arrangement used in many analogous settings, including free and open-source software,[75] and if drafted well, can be reliably expected to be upheld in court.[76] This additional transaction cost engineering would attempt to enable the provision of more robust services while also protecting ARIN from liability.

ARIN has taken some steps to adopt our recommendations. Specifically, it has created a new Redistributor RPA that specifically allows the distribution of machine-readable information based on RPKI for routing purposes to third parties provided that those third parties have either signed an RPA or a contract with the redistributor that includes terms that are at least as protective as the key terms of the RPA.[77] We note that the

[73] Yoo & Wishnick, *supra* note _, at _.
[74] *See, e.g.*, RESTATEMENT (SECOND) CONTRACTS §302 (1981).
[75] *See, e.g.*, *NASA Open Source Agreement v1.3 (NASA-1.3)*, OPEN SOURCE INITIATIVE, https://opensource.org/licenses/NASA-1.3 (last visited Dec. 27, 2018).
[76] *See* RESTATEMENT (SECOND) CONTRACTS § 302 (1981) (citing cases).
[77] American Registry for Internet Numbers, Ltd., Resource Certification Redistributor Relying Party Agreement § 9 (Oct. 2019), https://www.arin.net/resources/manage/rpki/rpa_redistributor.pdf.

Redistributor RPA may need some additional conforming changes. The prohibited conduct clause still retains language from the RPA prohibiting the redistribution of RPKI information for routing purposes.[78] We expect that this inconsistency will be cleaned up in future versions of the document. In the meantime, we trust that courts will honor the new provision on the principles that the specific controls the general and that the contract should be construed to give effect to the intention of the parties.[79]

This change represents another example of transaction cost engineering that should help reduce barriers to RPKI adoption. Again, its success depends on the details of contract drafting that cannot be bypassed by technology.

E. Linkage of RPKI to Other Issues (Including Property)

Up until now, we have focused on the agreement governing the validator side of RPKI. A separate set of agreements govern the signer side. In order to receive the cryptographic keys needed to sign ROAs, IP address holders that received their addresses after ARIN was created in 1997 must sign an agreement known as the Registration Services Agreement ("RSA"). IP address holders that received their addresses before ARIN was created must sign a Legacy Registration Services Agreement ("LRSA"). The RSA and LRSA (which now contain identical terms) cover the entire scope of a relationship between ARIN and a member, including RPKI. In addition, IP address holders that wish to sign ROAs must sign an RPKI Terms of Service Agreement. This agreement covers specific aspects of the ARIN-member relationship involving RPKI. Unlike the RPA, none of these agreements is browsewrap. Instead, they are explicitly signed by parties that wish to receive their RPKI keys.

The RPKI Terms of Service, RSA, LRSA all contain indemnification, arbitration, and choice of law clauses that may be outside the bounds of an agency's ability to contract. The solution here is identical to what was proposed above: ARIN and the NANOG community should publicize ARIN's policy of dropping both clauses for governmental entities that are barred by law or regulation from agreeing to them.[80] ARIN should also present the RPKI Terms of Service to new LRSA (and RSA) signatories

[78] *Id.* § 5.
[79] *See* Curran, *supra* note _ (indicating that the Redistributor RPA is intended to allow "qualified organizations . . to distribute RPKI-related data for purposes not covered in this standard RPA, *including but not limited to distribution for real-time routing purposes*" (emphasis added)).
[80] *See* ARIN RSA FAQ, *supra* note 53.

during the member onboarding process. This would save repeat visits between lawyers.

Legacy IP address raised more significant concerns about a different provision of the LRSA. Although legacy resource holders are entitled to receive the same services they were receiving before ARIN came into existence, ARIN requires them to sign the LRSA if they want to receive any new services, including RPKI. This requires the legacy address holders to agree to the "no property rights" clause "acknowledg[ing] and agree[ing] that" they lack property rights in their IP number resources.[81] Some legacy resource holders view this as an unreasonable concession due to their view that they hold rights that would be given away via such an acknowledgment. They view themselves as the owners or legitimate controllers of their legacy IP resources and do not want to run the risk of turning over any iota of their present control to ARIN.[82]

The perceived hindrance posed by the no property rights clause is real, but it is difficult to measure its impact. At present, the broader issue of legacy resource treatment is negatively impacting the comparatively narrow and logically distinct issue of RPKI adoption. Legacy resource holders that are interested in participating in RPKI but are apprehensive about signing ARIN's LRSA must decide which position they value more. Anecdotal evidence indicates that multiple parties faced with that tradeoff have opted to avoid RPKI. That is, the current linkage between the LRSA and RPKI access likely is not driving legacy holders to sign the LRSA. Rather, it is turning them away from RPKI.

We do not mean to overstate the importance of the LRSA. It is not clear whether the LRSA is a "but-for" cause of non-adoption. At present, most network operators that have signed LRSAs still have not deployed RPKI. The same is true for the IPv6 address spaces held by IPv4 legacy resource holders that signed RSAs in order to obtain their IPv6 address blocks. In addition, signing the LRSA may make it easier for legacy address holders to

[81] American Registry for Internet Numbers, Ltd., Registration Services Agreement § 7 (LRSA: version 4.0 Aug. 16, 2016), *available at* https://www.arin.net/about/corporate/agreements/rsa.pdf.

[82] Milton Mueller, *It's official: Legacy IPv4 address holders own their number blocks*, INTERNET GOVERNANCE PROJECT (Sept. 22, 2012), https://www.internetgovernance.org/2012/09/22/its-official-legacy-ipv4-address-block-holders-own-their-number-blocks/.

sell their addresses.[83] Lessening the perceived burden of the LRSA would hardly be a silver bullet. In addition, transfers of legacy IP space continue to reduce the set of legacy holders for whom the LRSA might be barrier. Nevertheless, it would be valuable to remove the LRSA as a roadblock on the path to widespread issuance of ROAs.

Given that cybersecurity and residual rights in addresses are conceptually distinct, it is worth exploring whether decoupling the issues could enable ARIN to better serve its goal of driving RPKI participation while respecting the rights of its full members and without reopening the contentious "property rights" issue. This would be especially valuable in North America, where there is a higher concentration of legacy IP holdings than in other regions. As a result, ARIN's decision to tie the RPKI to the LRSA poses a higher cost on RPKI adoption in North America than it would in other regions.

To achieve more widespread ROA-issuance, ARIN could consider altering its approach to the no property rights clause. The key role played by the no property rights clause in the LRSA is to create a structure that enables ARIN to provide registration services to LRSA signatories under conditions it sees as appropriate for operating its authoritative registry. The LRSA gives a party "[t]he exclusive right to be the registrant" of a given address block, and the "right to transfer the registration" within the ARIN registry under the terms of ARIN's governance.[84] This set of rights is paired with the no property rights clause concept to clearly establish ARIN's control over how transfers and registrations take place within its registry. One can think of the no property rights clause as one side of a deal and the rights of registration and transfer as the other side.

ARIN and its members should consider whether to decouple that entire deal from the RPKI Resource Certification process. That is, they should consider offering a transactional pathway to obtaining RPKI private keys that neither requires a "no property rights" admission, nor delivers any rights regarding registration or transfer of IP space. By separating RPKI from the property rights controversy, ARIN would open the RPKI door to LRSA holdouts. ARIN could adopt an at-will, fee-for-service model for this pathway, in which ARIN protects all its other rights as put forth in the

[83] Carolyn Duffy Marsan, *Does ARIN have the right to approve all IPv4 address sales?*, NETWORK WORLD (May 11, 2011, 5:00 AM PST), https://www.networkworld.com/article/2203104/does-arin-have-the-right-to-approve-all-ipv4-address-sales-.html.
[84] *Id.* § 2(b).

normal LRSA. Further, this clause could contain a provision allowing termination with explicit reversion to the status quo ante.

This would place ARIN closer to RIPE NCC and the Asia-Pacific Network Information Centre ("APNIC"). Both have constructed multiple pathways to receive RPKI services that do not require the signing of a full member services agreement.[85] For RIPE NCC, these include the options of (i) signing a "non-member service contract," (ii) contracting with a sponsoring Local Internet Registry, and (iii) seeking an accommodation for special circumstances.[86] Each of these pathways separates the question of access to RPKI keys from the broader question of a legacy resource holder's relationship with the RIR and requires those benefiting from RPKI services to compensate the RIR for the costs of making them possible. Thus, entities wishing to avoid an affirmative consent to the idea that they hold no property rights in registered IP resources (something also contained in RIPE NCC's Standard Services Agreement)[87] can opt for one of the alternate pathways.

Under a non-member service contract, legacy resource-holders could be ushered into the RPKI fold without having to overcome their deep-seated opposition to agreeing to the LRSA. In such a contract, ARIN could retain broad rights to deliver or terminate RPKI services and support to parties unwilling to sign the LRSA. In essence, such a structure would give ARIN an ongoing option to deliver RPKI services to non-signatories of the LRSA. This could help bring more participants into the ROA process. The attractiveness of this approach would depend on the interest and willingness of paid-in ARIN members to facilitate greater service-provision to those not yet signed up.

The creation of alternative pathways represents another form of transaction cost engineering that could facilitate the deployment of RPKI. The controversy over the no property rights clause is not animated by the need to strike a balance between supporting the operation and growth of the Internet on the one hand and protecting ARIN from tort liability on the

---

[85] *See APNIC Non-Member Resource Services Agreement*, APNIC (July 1, 2002), https://www.apnic.net/about-apnic/corporate-documents/documents/membership/non-member-agreement/; *RIPE NCC Services to Legacy Internet Resource Holders*, RIPE NCC (Mar. 16, 2015), https://www.ripe.net/publications/docs/ripe-639; *Policy for Resource Certification for Non-RIPE NCC Members*, RIPE NCC (Oct. 16, 2013), https://www.ripe.net/publications/docs/ripe-596.

[86] *See RIPE NCC Services to Legacy Internet Resource Holders*, RIPE NCC, at § 2 (Mar. 16, 2015), https://www.ripe.net/publications/docs/ripe-639.

[87] *See RIPE NCC Standard Services Agreement*, RIPE NCC, at § 10.2 (Dec. 27, 2016), https://www.ripe.net/publications/docs/ripe-673.

other. Instead, it represents tying RPKI into its efforts to achieve other objectives unrelated to these goals. This raises the possibility of classic principal-agency problems that often arise in nonprofit organizations.[88] At a minimum, it introduces a source of friction into the RPKI adoption process that is completely divorced from RPKI. This too constitutes transaction cost engineering but one designed to reduce friction in the transaction at hand but rather to harness it to further other unrelated ends.

* * *

Taken together, these findings show that RPKI's adoption was hindered by the contractual governance choices embodied in ARIN's RPA. Contract terms prevented some potential adopters from experimenting with the RPKI technology even in test environments, to say nothing of implementing it into production networks. Others were chilled from proposing that their organizations adopt the technology. For some, the mechanism was fear of exceeding their authority by assenting to contract terms outside their firms' standard policy bounds. Others feared assenting to any agreement at all. Still others did not wish to invest the effort associated with bringing lawyers into the technology-adoption decision. In each case, contractual governance decisions had real consequences affecting the technology-adoption calculus.

V. BEYOND CONTRACT: ORGANIZATIONAL DESIGN AS A SOURCE OF TRANSACTION COST ENGINEERING

The primary focus of this Article has been on the role of contract in transaction cost engineering. Scholars have long recognized that organizational and institutional design can also play an important role in reducing the friction that can impede the realization of socially beneficial outcomes.[89] This is particularly the case when network effects are involved.[90]

[88] *See, e.g.*, Richard Steinberg, *Principal-Agent Theory and Nonprofit Accountability*, *in* COMPARATIVE CORPORATE GOVERNANCE OF NON-PROFIT ORGANIZATIONS 73 (Klaus J. Hopt & Thomas Von Hippel eds., 2010) (surveying the literature).

[89] *See, e.g.*, OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM 397-404 (1985).

[90] *See, e.g.*, DANIEL F. SPULBER & CHRISTOPHER S. YOO, NETWORKS IN TELECOMMUNICATIONS: ECONOMICS AND LAW 138-43 (2009) (surveying how private ordering and alternative institutional forms can overcome barriers to adoption created by network effects).

A. The Role of Institutional Actors

For example, the decisions of large actors can increase incentives to adopt RPKI to a sufficient extent to overcome transaction cost obstacles, particularly in markets with network effects where the decision of a large player can go a long way to achieving the necessary critical mass.[91] As noted above, key market players such as AT&T, Cloudflare, Google, Comcast, and major IXPs have boarded the RPKI bandwagon.[92] These decisions can provide additional impetus toward adoption that can help overcome the remaining transaction cost obstacles, particularly if they begin encouraging their partners and suppliers to adopt RPKI.

Perhaps the biggest actor yet to move is the U.S. federal government. As one of the most significant purchasers of network services, any decision other part would provide strong motivation for RPKI adoption. NIST has published documents encouraging broader use of RPKI.[93] History has shown that the Office of Management and Budget ("OMB") has been the catalyst for adopting new technologies, such as IPv6, in the past.[94] Other voices have joined our call for OMB to make a similar move with respect to RPKI.[95]

B. The Possibilities of Exit and Voice

To borrow Albert Hirshman's famous framework, other alternatives include exit and voice.[96] In terms of voice, the technical community and interested actors in private industry and government continue to work within existing deliberative processes to make changes that would facilitate RPKI. Indeed, the engagement prompted by this research has already prompted modifications that should lower transaction costs. The likely success of such efforts is determined in large part by the processes each RIR has adopted for community deliberation and decisionmaking. Comments on the influence that key differences in the processes employed by RIPE NCC and ARIN bear further study.

---

[91] *Id.* at 140-41.
[92] *See supra* notes _ and accompanying text.
[93] HAAG ET AL., *supra* note 25.
[94] Yoo & Wishnick, *supra* note _, at 32-33.
[95] JUSTIN SHERMAN, THE POLITICS OF INTERNET SECURITY: PRIVATE INDUSTRY AND THE FUTURE OF THE WEB 23 (Atl. Council Scowcroft Ctr. for Strategy & Sec. Oct. 2020), https://www.atlanticcouncil.org/wp-content/uploads/2020/09/The-Politics-of-Internet-Security.pdf (adopting the recommendation in Yoo & Wishnick, *supra* note _, at 33).
[96] ALBERT O. HIRSHMAN, EXIT, VOICE, AND LOYALTY (1970).

With respect to exit, the conventional wisdom has been that the fact that each geographic region is governed by a single RIR has effectively removed it as an option. Although RIRs have processes for transferring oversight of *unused* IPv4 addresses to another RIR,[97] Recent postings have begun to explore the possibility of transferring IP addresses that are *in use* to the RIR overseeing a different region.[98] This dynamic could give rise to the type of "voting with your feet" that now characterizes the de facto competition among global stock exchanges.[99] These possibilities do not necessarily have to be exercised in order to be effective.

C. The Expectations and Preparedness of the Community

Finally, the success of RPKI adoption depends on the operational readiness of the entire Internet ecosystem. Indeed, many interviewees emphasized that widespread RPKI adoption must be accompanied by high levels of operational competence to ensure that RPKI is a source of security, and not a source of newly-introduced problems.

Interviewees who raised this theme tended to coalesce around three main points. First, network operators that begin making routing decisions based on RPKI information must adopt best practices when they do so. They must prepare to handle outages on the part of the RIRs, and they must be ready to failover gracefully. As noted earlier, no informational service is reliable and available 100% of the time, and RPKI is no exception. As a result, all network operators must ensure that their networks are resilient in the face of unavailable RPKI publication points and other problems that may arise despite every participant's best efforts. Indeed, on June 2, 2021, ARIN disclosed that it will test network operators' readiness to deal with a repository failure by shutting it down for thirty minutes at an unannounced time.[100]

Second, interviewees stated that network operators would benefit from greater clarity regarding how the five RIRs intend to deliver their RPKI services. Interviewees reported that standardized and expanded disclosures

---

[97] *See, e.g.*, *Transferring IP Addresses & ASNs*, ARIN, https://www.arin.net/resources/registry/transfers/#inter-rir-transfers (last visited Sept. 26, 2021).

[98] *FAQ*, READ THE DOCS, https://rpki.readthedocs.io/en/latest/about/faq.html (last visited Sept. 26, 2021).

[99] *See, e.g.*, Chris Brummer, *Stock Exchanges and the New Markets for Securities Las*, 75 U. CHI. L. REV. 1435 (2008).

[100] Brad Gorman, *Notice of upcoming maintenance to ARIN's RPKI infrastructure*, ARIN (June 2, 2021), https://www.arin.net/announcements/20210602-rpki/.

of service-level intentions among the RIRs would enable network operators to better prepare themselves for foreseeable contingencies when relying on RPKI.

Third, RIRs must prepare to provide real-time support for RPKI services. This may require significant changes to RIR operations, as they have primarily issued resources and overseen changes that were not as time sensitive. RIRs must undertake efforts to understand precisely what support RPKI users need and on what timing and to disclose their plans of how to meet those expectations.

Although evaluation of particular best practices and service-level intentions among operators and RIRs is beyond the scope of this report, the general lesson is essential: it is far more valuable to *reduce* risks than to allocate them via well-crafted legal arrangements. At its best, good legal design can incentivize risk reduction, but the lion's share of risk reduction will depend on the initiative and ingenuity of engineers and technical staff at network operators and at the RIRs. This makes clear that transaction cost engineering can operate not just on the transaction itself but also on the environment surrounding the contract.

CONCLUSION

The quality of a technical standard not only depends on its functional design, but also on the broader forces—political, social, economic, legal—that determine its attractiveness to potential adopters. In this Article, we have argued that contractual and organizational lawyering can be significant. To do so, we analyzed legal materials and interviews with participants in the industrial governance network for Internet security regarding the case of the RPKI standard. Our analysis reveals that contracts and organizational governance have played an important role. These private-law forces have limited complementary innovation and chilled non-lawyer technologists from engaging their employers in the RPKI project. At the same time, private legal arrangements have also prompted dialogue among key stakeholders regarding RPKI's implementation and attendant risks. Even in the most technical realms of Internet operation, law has mattered—and private law, at that. While RPKI is only one standard, the case study suggests that scholars will benefit from looking beyond intellectual property and public regulation when examining law's role in standards adoption.