
14-7193

**IN THE
UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT**

SUSAN WEINSTEIN, individually, Co-Administrator of Estate of Ira William
Weinstein, and natural guardian of plaintiff DAVID WEINSTEIN; JEFFREY A. MILLER,
Co-Administrator of Estate of Ira William Weinstein; JOSEPH WEINSTEIN; JENNIFER
WEINSTEIN HAZI; DAVID WEINSTEIN, minor, by guardian and next friend SUSAN
WEINSTEIN,
Petitioners-Appellants,

v.

ISLAMIC REPUBLIC OF IRAN; IRANIAN MINISTRY OF INFORMATION AND SECURITY;
AYATOLLAH ALI HOSEINI KHAMENEI, Supreme Leader of the Islamic Republic of
Iran; ALI AKBAR HASHEMI-RAFSANJANI, Former President of the Islamic Republic of
Iran; ALI FALLAHIAN-KHUZESTANI, Former Minister of Information and Security,
Defendants,

and

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS,
Appellees.

Consolidated with Nos. 14-7194, 14-7195, 14-7198, 14-7202, 14-7203 and 14-7204

**PETITIONERS-APPELLANTS' PETITION FOR
PANEL REHEARING AND REHEARING *EN BANC***

Petitioners-Appellants
by their Attorneys,

Steven T. Gebelin
Scott M. Lesowitz
RAINES FELDMAN LLP
9720 Wilshire Boulevard, 5th Floor
Beverly Hills, California 90212
(310) 440-4100
sgebelin@raineslaw.com
slesowitz@raineslaw.com

Robert J. Tolchin
Meir Katz
THE BERKMAN LAW OFFICE, LLC
111 Livingston Street, Suite 1928
Brooklyn, NY 11201
(718) 855-3627
rtolchin@berkmanlaw.com
mkatz@berkmanlaw.com

CERTIFICATE AS TO PARTIES AND AMICI CURIAE

Pursuant to Circuit Rules 28(a)(1)(A) and 35(c), Petitioners-Appellants Weinstein *et al.* (“petitioners”) hereby certify as follows:

(A) Parties and Amici. The following is a list of persons who are known to be parties to this case at this time:

Petitioners-Appellants-Plaintiffs: Susan Weinstein, individually as Co-Administrator of the Estate of Ira William Weinstein, and as natural guardian of plaintiff D.W.; Jeffrey A. Miller, as Co-Administrator of the Estate of Ira William Weinstein; Joseph Weinstein; Jennifer Weinstein Hazi; D.W., minor, by his guardian and next friend Susan Weinstein; Shaul Stern, individually and as legal representative of the Estate of Leah Stern; Joseph Stern; Shimson Stern; Yocheved Kushner; Jenny Rubin; Deborah Rubin; Daniel Miller; Abraham Mendelson; Stuart Elliot Hersh; Renay E. Frym; Noah Rozenman; Elena Rozenman; Tzvi Rozenman; Seth Charles (Klein) Ben Haim; Bernard (Klein) Ben Haim; Lavi (Klein) Ben Haim; Ruth Calderon-Cardona; Luz Calderon-Cardona; Luis Calderon-Cardona; Gloria Calderon-Cardona; Jose Raul Calderon-Cardona; Ana Delia Calderon-Cardona; Hilda Calderon-Cardona; Angel Calderon-Guzman; Miguel Calderon-Guzman; Salvador Calderon-Martinez; Pablo Tirado-Ayala; Antonia Ramirez-Fiero; Mary Nell Wyatt, individually and as executrix of the Estate of Ronald E. Wyatt; Daniel Wyatt; Amanda Lippelt; Michelle Brown; Marvin T. Wilson; Renetta Wilson; Marty R. Wilson; Gina R. Brown; Bradley

G. Key; Kimi L. Johns; and Barry T. Key. None of the petitioners has a parent company and no publicly-held company has a 10% ownership interest in any of the petitioners.

Defendants-Judgment Debtors: The following were Defendants in their respective underlying cases, but did not participate before the district court in this action and are not parties to this appeal: the Islamic Republic of Iran; the Iranian Ministry of Information and Security; Ayatollah Ali Hoseini Kharnenei, Supreme Leader of the Islamic Republic of Iran; Ali Akbar Hashemi-Rafsanjani, Former President of the Islamic Republic of Iran; Ali Fallahian-Khuzestani, Former Minister of Information and Security; Palestine Islamic Jihad, also known as Palestine Islamic Jihad-Shaqaqi Faction, also known as, Palestinian Islamic Jihad, also known as, Islamic Jihad of Palestine, also known as Harakat Al-Jihad Al-Islami Al-Filastini; the Democratic People's Republic of Korea; the Cabinet General Intelligence Bureau; and the Syrian Arab Republic.

Third Party Garnishees-Appellees: Internet Corporation for Assigned Names and Numbers ("ICANN").

Dismissed Defendants: The Kurdistan Workers Party (also known as the PKK) was a defendant in *Wyatt, et al. v. Syrian Arab Rep.*, No. 1:08-cv-00502 (D.D.C.), but was dismissed from that action.

Intervenors & Amici: The United States intervened in a couple of these consolidated actions while before their respective district courts and is *amicus curiae* before this Court. There are no other intervenors or amici pertinent to this appeal.

Table of Contents

CERTIFICATE AS TO PARTIES AND AMICI CURIAE..... *i*

TABLE OF AUTHORITIES *iii*

BACKGROUND.....2

ARGUMENT

I. Binding precedent demands remand and discovery, not speculation and “imagin[ation],” regarding the protection of any third-party interests6

II. 28 U.S.C. 1610(g)(3) does not prohibit attachment in the face of third party interests, it merely acknowledges the existence of background protections.....10

III. Petitioners did not waive their attachment of the IP addresses11

IV. Petitioners did not forfeit the enforcement of their writs13

CONCLUSION.....15

ADDENDUM

Table of Authorities

Cases

<i>Bennett v. Islamic Rep. of Iran</i> , 825 F.3d 949 (9th Cir. 2016).....	6
<i>Consumers United Ins. v. Smith</i> , 644 A.2d 1328 (D.C. 1994).....	8, 11
<i>CRS Recovery v. Laxton</i> , 600 F.3d 1138 (9th Cir. 2010).....	5
<i>Curtiss-Wright v. GE</i> , 446 U.S. 1 (1980)	9
<i>Envtl. Def. Fund v. E.P.A.</i> , 210 F.3d 396 (D.C. Cir. 2000).....	1, 15
<i>Exxon Shipping v. Baker</i> , 554 U.S. 471 (2008)	15
<i>Fairey v. Tucker</i> , 132 S.Ct. 2218 (2012)	12
<i>In re Harman Int’l Indus.</i> , 791 F.3d 90 (D.C. Cir. 2015).....	1, 9
<i>Hudson Ins. v. Kumari</i> , ___ F.Supp.3d ___, 2016 WL 3248192 (D.D.C. 2016).....	8
<i>Hudson United Bank v. LiTenda Mortgage</i> , 142 F.3d 151 (3d Cir. 1998).....	9
<i>Kremen v. Cohen</i> , 337 F.3d 1024 (9th Cir. 2003).....	5
<i>Office Depot v. Zuccarini</i> , 596 F.3d 696 (9th Cir. 2010).....	5
<i>Peterson v. Islamic Rep. of Iran</i> , 627 F.3d 1117 (9th Cir. 2010).....	13-14

<i>Rubin v. Islamic Rep. of Iran</i> , 637 F.3d 783 (7th Cir. 2011)	13-14
<i>In re Sealed Case</i> , 121 F.3d 729 (D.C. Cir. 1997).....	1, 12-13
<i>Singleton v. Wulff</i> , 428 U.S. 106 (1976)	1, 9
<i>Sprinkler Warehouse v. Systematic Rain</i> , 880 N.W.2d 16 (Minn. 2016)	5
<i>Summers v. DOJ</i> , 140 F.3d 1077 (D.C. Cir. 1998).....	9
<i>Texas Rural Legal Aid v. Legal Servs.</i> , 940 F.2d 685 (D.C. Cir. 1991).....	9
<i>Thomas v. Network Sols</i> , 176 F.3d 500 (D.C. Cir. 1999).....	1, 9
<i>Tucows.com v. Lojas Renner</i> , 2011 ONCA 548 (Ct. App. Ontario 2011)	5
<i>U.S. v. Olano</i> , 507 U.S. 725 (1993)	12-14
<i>U.S. v. Peyton</i> , 745 F.3d 546 (D.C. Cir. 2014).....	9
<i>U.S. v. Van Smith</i> , 530 F.3d 967 (D.C. Cir. 2008).....	1, 15
<i>Wainwright v. Sykes</i> , 433 U.S. 72 (1977)	13
<i>Washburn v. Lavoie</i> , 437 F.3d 84 (D.C. Cir. 2006).....	15
<i>Washington Loan & Trust v. Susquehanna Coal</i> , 26 App. D.C. 149 (D.C. Cir. 1905)	1, 8, 11

Statutes

28 U.S.C.:

§ 16052

§ 1605A2

§ 16102, 5-6, 10-11, 13

Terrorism Risk Insurance Act of 2002 (“TRIA § 201”), Pub. L. 107-297,
 title II, § 201, 116 Stat. 2337, 2339 (2002) (codified at 28 U.S.C. § 1610
 note)5, 13

D.C. CODE:

§ 16-51911

§ 16-52311

§ 16-52811

§ 16-5443, 5

§ 16-55111

Rules

Fed. R. Civ. P.:

Rule 122

Rule 693, 11

Other Authority

H.R. Conf. Rep. No. 110-477 6, 10-11

Petitioners respectfully petition for panel rehearing and rehearing *en banc* of the Court's Opinion of August 2, 2016.¹ Rehearing is necessary because the panel's decision 1) conflicts with *Singleton v. Wulff*, 428 U.S. 106, 120-21 (1976); *Washington Loan & Trust v. Susquehanna Coal*, 26 App. D.C. 149, 153-54 (D.C. Cir. 1905); *In re Sealed Case*, 121 F.3d 729, 740-41 (D.C. Cir. 1997); *U.S. v. Van Smith*, 530 F.3d 967, 970 n.2 (D.C. Cir. 2008); *Env'tl. Def. Fund v. E.P.A.*, 210 F.3d 396, 401 n.8 (D.C. Cir. 2000); *In re Harman Int'l Indus.*, 791 F.3d 90, 100-01 (D.C. Cir. 2015); *Thomas v. Network Sols*, 176 F.3d 500, 510 (D.C. Cir. 1999) (Randolph, J.), and numerous other decisions of this Court, and 2) involves legal questions of exceptional importance in that it a) significantly alters the doctrine governing attachment of third-party assets, b) prevents the attachment of Internet domain names in the District of Columbia, c) significantly impairs the ability of victims of terrorism to enforce terrorism-related judgments, d) massively expands the doctrines of waiver and forfeiture, e) reaches numerous profound questions of law despite acknowledging that it opines on questions not reached below, in the absence of a full record, and in reliance on its own speculation, f) undermines reasonable efforts by the district courts to address elements of a case in piecemeal fashion, and g) rests on significant factual errors.

The only relief that petitioners sought from this Court was remand for discovery so that the significant legal questions raised herein could be properly considered. The panel of two judges² refused. Relying on conjecture, it significantly solidified

¹ A copy is attached in the Addendum and referenced throughout as "Op."

² See Op. 2 n.* (noting that Chief Judge Garland did not participate in the opinion).

ICANN's monopoly over Internet governance (antagonizing many small Internet participants who have been bullied by ICANN over many years), massively altered the waiver doctrine, impaired the operation of 28 U.S.C. 1610(g), and injured judgment creditors who must recover their judgments from third-party garnishees.

The opinion also suffers from procedural peculiarities. In footnote 1, the panel claims to treat the matter on appeal as though it arises from a Rule 12(b)(6) motion, accepting petitioners' submissions as true. Op. 3 n.1. It went on to resolve this appeal by making numerous material factual assumptions regarding the operation of the Internet, despite the absence of factual support in the record or any significant discovery. Further, it held an issue waived, notwithstanding that petitioners raised that issue in their writs of attachment (the procedural equivalent of a civil complaint) and the appellees failed to challenge it in their motions to quash (the equivalent of a motion to dismiss). Finally, rather than making inferences in petitioners' favor, the panel discredited their representations regarding the lack of discovery and the nature of their non-substantive preliminary "response" to a motion before the district court.

BACKGROUND

Petitioners are victims of terrorism holding money judgments (entered under 28 U.S.C. 1605(a)(7); 1605A) totaling hundreds of millions of dollars against the governments of Iran, North Korea, and Syria, for their roles in sponsoring and supporting terrorist attacks. Petitioners' judgments remain unsatisfied.

Petitioners argue that ICANN, a third-party, holds significant valuable assets of the judgment debtors and/or attachable interests therein. Specifically, petitioners argue that

the ccTLDs (for an explanation, see Op. 4-6; Appellants' Br. 5-9³) .IR, .SY, .KP, and their Arabic and Farsi equivalents, and the internet protocol ("IP") addresses of Iran, North Korea, and Syria (collectively, the "Property") are attachable and that ICANN is a garnishee of the Property. They further argue that D.C. CODE § 16-544, applicable under Fed. R. Civ. P. 69, authorizes attachment here. In June 2014, they served writs of attachment on ICANN, seeking the judgment debtors' interests in the Property and to operate the Property (likely through a designee) competently and professionally. *See* SA69-SA75.⁴ The writs, read together with their accompanying cover letters, expressly attach all of the Property, including the IP address. SA70.

On July 29, 2014, ICANN moved to quash the writs, making sundry arguments resting on its favored resolution of complicated factual questions. A22-A23. In its memorandum in support, ICANN makes numerous references to the ccTLDs but virtually none to the IP addresses; it mentions only the "supporting IP addresses" of the ccTLDs, oddly ignoring the fact that *all* of the judgment debtors' assigned IP addresses had been attached. SA70; *Weinstein*,⁵ DE 89-1 at *i* & 2. ICANN submitted certain cherry-picked documents as exhibits, but otherwise refused to participate in discovery in good faith. *See* Reply Br. 6-14; SA82-SA89 (demanding a court order before considering whether to release obviously discoverable relevant material); A45-A47. While petitioners could not reasonably respond without a factual record to support

³ One of Iran's ccTLD manifests as the .IR in "www.example.ir". It is, in a sense, Iran's space on the Internet.

⁴ Motion for leave to file supplemental appendix granted on December 18, 2015.

⁵ References to "*Weinstein*" are to district court docket No. 00-cv-2601 (D.D.C.).

their responses, their own limited informal investigation revealed that many of ICANN's representations to the district court were false and/or misleadingly incomplete. Appellants' Br. 15-16; A46-A47. Accordingly, on September 28, 2014, they requested by motion a six-month discovery period and an extension of time in which to respond to the motions to quash. A31-A33. They explained precisely what they desired to accomplish during their six-month discovery period, as is summarized in the opening brief. Appellants' Br. 16-18; A39-A41. Two days later, concerned that the district court might otherwise assume that ICANN's motions to quash went unopposed, the petitioners filed a place-holder "preliminary response" to the motions to quash that was obviously not intended as a substantive response. A59-A61. That place-holder, not two full pages long, referenced the pending discovery motion (which was attached as an exhibit) and the pending request for an extension of time and did nothing but explain why discovery was a necessary prerequisite to a response on the merits. While the place-holder "response" made no specific reference to IP addresses ("supporting" or otherwise), the attached discovery motion did. A51-A52; A59-A61; *Weinstein*, DE 107 at 5, 7⁶, 9.⁷

On November 10, 2014, the district court attempted to resolve this litigation without reaching the many unresolved factual questions. It held, as a matter of first impression,

⁶ "ICANN has presented virtually no facts concerning its role in the distribution of IP addresses or the ownership and value of IP addresses." Discovery Mtn. at 7.

⁷ "ICANN's Motion to Quash does not address the economic value of IP addresses, a separate asset, which...raises its own factual questions requiring further discovery." Discovery Mtn. at 9.

that D.C. CODE § 16-544 does not permit the attachment of Internet domain names. A71-A73. In so holding, the district court diverged from every court to consider the question in recent years, rendering D.C. law an outlier. *See Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003); *Office Depot v. Zuccarini*, 596 F.3d 696, 701-702 (9th Cir. 2010); *CRS Recovery v. Laxton*, 600 F.3d 1138, 1142-43 (9th Cir. 2010); *Sprinkler Warehouse v. Systematic Rain*, 880 N.W.2d 16, 18-24 (Minn. 2016);⁸ *Tucows.com v. Lojas Renner*, 2011 ONCA 548, ¶¶ 41-66 (Ct. App. Ontario 2011)⁹ (Ontario's high court). The district court made no finding as to how D.C. law would address attachment of IP addresses. It nevertheless quashed the writs of attachment without differentiation. A63-A65, A71-A73.

The panel affirmed on alternative grounds, declining to reach D.C. CODE § 16-544. In so doing, it kept in place the district court's decision that could serve to frustrate the application of § 16-544 in cases well beyond this one, holding that Internet domain names are not attachable under D.C. law.

Instead, the panel found that petitioners waived their attachment of the IP addresses and forfeited their arguments for enforcement under TRIA § 210 and 28 U.S.C. 1610(a)(7). Op. 25-27. It further held that because § 1610(g) does not “*supersede* the authority of a court to prevent appropriately the impairment of an interest held by a person who is not liable,” § 1610(g)(3) (emphasis added), the mere possibility that third-party interests might be impaired precludes attachment. *See* Op. 28-33.

⁸ *See* FRAP 28(j) letter filed March 28, 2016.

⁹ *See* FRAP 28(j) letter filed January 18, 2016.

ARGUMENT

I. Binding precedent demands remand and discovery, not speculation and “imagin[ation],” regarding the protection of any third-party interests

After asserting the “authority” to prevent impairment to third-party interests that might be occasioned in an attachment, and noting that, under different circumstances, remand would be warranted, the panel asserts that because “there is *no* way to execute on the plaintiffs’ judgments without impairing” third-party interests, it “*cannot* permit attachment.” Op. 27-29 (first emphasis in original). It erred on the latter point and made no effort to demonstrate the former (it cannot), instead speculating that attachment *might* impair third-party interests.

The latter point—that this Court and the district court are rendered *powerless* by § 1610(g)(3)—is easily refuted. Nothing in § 1610(g)(3) *requires* a court to block an attachment whenever it perceives that the attachment will impair the interests of a third party. Rather, it instructs courts that they *may* “appropriately” protect third-party interests. § 1610(g)(3). The statute thus calls for an exercise of discretion made in light of all of the facts and circumstances, “on a case-by-case basis,” as to whether and how to intervene so as to prevent the impairment of third party interests. *See* H.R. Conf. Rep. No. 110-477, at 1002; *Bennett v. Islamic Rep. of Iran*, 825 F.3d 949, 962 (9th Cir. 2016) (holding that § 1610(g)(3) vests the district court with “discretion” to act or to decline to act). Just as with any exercise of discretion, it demands a close understanding of the facts and circumstances.

Assessing the pertinent facts and circumstances, the panel described the various ways in which it *assumed* that attachment would impair third-party interests:

1) attachment would cause the Property to be mismanaged, if the petitioners' designee were incompetent to manage it, 2) the process by which ICANN delegates ccTLDs would be bypassed, potentially undermining ICANN's ability to protect the stability of the Internet; 3) redelegation of the ccTLDs to the petitioners' designee might not automatically cause all of the websites registered with those ccTLDs to be registered with the petitioners' designee (who would then be operating the ccTLDs), thus impairing the interests of those website owners and end-users attempting to visit them; and 4) attachment imposes the mere *possibility* of splitting the Internet "root," which could undermine the Internet's operation. Op. 29-33. But none of the panel's concerns is supported by the record or even likely to impair a third-party's interests.

First, petitioners stated both in their reply brief (Reply Br. 26-27) and at oral argument that the Property will be managed by a competent manager, under the supervision of the district court. Nothing in the record counters that representation. It is precisely the type of representation that this Court should credit in accepting the petitioners' factual allegations as true and granting them the benefit of every reasonable inference. *See* Op. 3 n.1. In any event, the petitioners have no expectation that the district court would permit transfer of the Property absent assurances that the operator of the Property is competent. Finding competent parties to operate the ccTLDs will be quite easy given that there exists a functioning marketplace for the management of TLDs.

Second, that ICANN's process of delegating ccTLDs would be bypassed is irrelevant and would have—at worst—only a trifling temporary impact on Internet stability.

ICANN is a third-party garnishee. By definition, any third-party garnishee (and its assignees) has an interest in property sought to be attached. In a typical garnishment, the garnishee physically possesses money or other tangible assets of the judgment debtor. Here, ICANN benefits from maintaining the current assignments of the Property, thus entrenching its authority as governor of the Internet. Yet the very fact that garnishment from third parties is permitted means that such “interests” are discounted in the face of a primary lien of a judgment creditor. *Washington Loan*, 26 App. D.C. at 153-54; *Consumers United Ins. v. Smith*, 644 A.2d 1328, 1348-52, 1355-56 (D.C. 1994); *Hudson Ins. v. Kumari*, ___ F.Supp.3d ___, 2016 WL 3248192 at *2 (D.D.C. 2016). Petitioners do not seek any legitimate property interest that fairly belongs to ICANN.

The separate contention that even a slight disruption of ICANN’s monopoly over Internet governance would itself disrupt the Internet is nothing but pure conjecture, lacking even a scintilla of support in the record. It is no basis to deny *discovery*.

Third, as petitioners stated at oral argument, the re-delegation will likely be seamless and noticeable to no one other than website owners themselves and *only* when they pay their annual fee. *Contra Op.* 30-31. Could the current managers of the ccTLDs refuse to cooperate? Certainly, to the extent that their cooperation is necessary to retrieve information beyond publicly available routing information for existing subdomain holders. But that is no insurmountable problem. The panel’s contrary *assumption*—without any record evidence—is remarkable.

Fourth, in asserting that attachment here might split the root, the panel admitted that

it was speculating. It found its speculation “not beyond imagining” and thereby prohibited any discovery that might have obviated the need for such imagination. Op. 33. The panel’s fears are exceptionally unlikely to come to fruition. In any event, remanding the case to permit *discovery* carries with it no risk of splitting the root and would help to determine the extent of that risk, *vel non*.

Normally, this Court—a “court of review, not of first view.” *U.S. v. Peyton*, 745 F.3d 546, 557 (D.C. Cir. 2014)—does not pass on questions not reached below, absent “exceptional circumstances.” *Thomas*, 176 F.3d at 510; *In re Harman*, 791 F.3d at 100-01; *Summers v. DOJ*, 140 F.3d 1077, 1083-84 (D.C. Cir. 1998); *Texas Rural Legal Aid v. Legal Servs.*, 940 F.2d 685, 697-98 (D.C. Cir. 1991) (refusing to reach an issue after noting that a party “did not address the merits of the claim at all, urging only that we remand...for discovery and factfinding”); *see also* Reply Br. 3-7 (collecting cases); *Hudson United Bank v. LiTenda Mortgage*, 142 F.3d 151, 159 (3d Cir. 1998) (“When the resolution of an issue requires the exercise of discretion or fact finding, ...it is inappropriate and unwise for an appellate court to step in.”); *Curtiss-Wright v. GE*, 446 U.S. 1, 10 (1980) (“[T]he proper role of the court of appeals is not to reweigh the equities or reassess the facts but to make sure that the conclusions derived...are juridically sound and supported by the record.”). Passing on new issues when “injustice was more likely to be caused than avoided” is an abuse of discretion. *Singleton*, 428 U.S. at 121; *see also id.* at 120. No exceptional circumstances justified the panel’s reaching questions neither reached nor fully briefed below, on an incomplete record, and without discovery. Reaching such issues prejudiced petitioners far more than

requiring ICANN to participate in discovery could have.

II. 28 U.S.C. 1610(g)(3) does not prohibit attachment in the face of third party interests, it merely acknowledges the existence of background protections

The panel somehow found in § 1610(g)(3) an *obligation* to block petitioners' attachments upon concluding that the interests of third parties might be impacted by those attachments. Op. 27-33. But § 1610(g)(3) does not so obligate the Court; it does nothing other than affirm the courts' pre-existing authority to protect the interests of third parties. Indeed, on its face, it effects nothing new at all:

Nothing in this subsection shall be construed to supersede the authority of a court to prevent appropriately the impairment of an interest held by a person who is not liable in the action giving rise to a judgment in property subject to attachment in aid of execution....

§ 1610(g)(3) (emphasis added). Legislative history confirms that Congress intended only to avoid the inference that a pre-existing rule was being abrogated:

While the provision is written to subject any property interest in which the foreign state enjoys a beneficial ownership to attachment and execution, the provision would *not supersede* the court's authority to appropriately prevent impairment of interests in property held by other persons who are not liable to the claimants.... The court would...*retain its authority* to take whatever steps it finds warranted to preserve the value of [a] business enterprise in which a third party may be a joint venture partner, for example.

H.R. Conf. Rep. No. 110-477, at 1001-02 (2007) (emphasis added). That Conference Report reveals the background law on which Congress relied and provides a specific example as to how a court might "prevent impairment" of third-party interests:

The conferees encourage the courts to protect the property interests of such innocent third parties by using their *inherent authority*, on a case-by-case basis,

under the *applicable procedures governing execution on judgment and attachment* in anticipation of judgment.

Id. at 1002 (emphasis added). D.C. statute, applicable here under Rule 69, provides “applicable procedures” to protect third-party interests in garnishment proceedings. *See, e.g.*, D.C. CODE §§ 16-519, 16-523, 16-528, 16-551. The court’s ability to protect third-party interests thus derives either from D.C. municipal statute or from its inherent authority, not § 1610(g)(3).

Because the application of third-party protections rests in D.C. municipal law and the court’s inherent authority, not § 1610, the panel’s holding is not limited to § 1610 cases. Given that holding, courts must block a garnishment *whenever* there is an unsubstantiated and unexplored risk that permitting the attachment *might* diminish a third-party interest. But that is *not* the law in D.C. *Washington Loan*, 26 App. D.C. at 153-54; *Consumers United*, 644 A.2d at 1348-52. The panel’s holding is erroneous.

III. Petitioners did not waive their attachment of the IP addresses

There can be no dispute that the petitioners properly attached the judgment debtors’ IP addresses and adequately placed ICANN on notice that the IP addresses had been attached. SA69-SA75. ICANN plainly misapprehended the scope of the attachment, moving to quash only the attachment against those IP addresses that support the judgment debtors’ operation of their ccTLDs, failing to raise any argument regarding any other IP addresses. *See Weinstein*, DE 89-1 at *i* & 2. Thus, no motion was presented to the district court to quash the attachment of the remaining IP addresses. It did so, without allowing discovery, in an abuse of discretion. *See Appellants’ Br.* 43.

Petitioners preserved their arguments on this point by raising them on appeal. *Id.* at 1, 3-5, 9-11, 17-21, 23, 25, 37, 43-47.

The panel nonetheless held that because petitioners' response to the district court mentioned the IP addresses "only twice" but mentioned the ccTLDs "78 times," the district court acted within its discretion in dismissing the attachment of the IP addresses. Op. 26-27. Waiver is not so lightly presumed. *See In re Sealed Case*, 121 F.3d at 740-41; *Fairey v. Tucker*, 132 S.Ct. 2218, 2220 (2012). Here, the very fact that the petitioners attached the IP address (SA70) and mentioned that attachment in their court filings is sufficient to avoid waiver of that attachment. Regardless, ICANN never moved to quash the attachment of the IP addresses. Accordingly, petitioners had no need to address them in response to ICANN's motion; that petitioners did not discuss the IP addresses at length is unremarkable.

The panel additionally chided petitioners for not directly responding to the government, which (the panel asserts) expressed doubt that petitioners had preserved arguments regarding the IP addresses. Op. 27.¹⁰ The panel thus held those arguments "waived." *Id.* But petitioners had no need to respond to the government directly, having previously raised and adequately defended those arguments in earlier briefing. Appellants' Br. 1, 3-5, 11, 17-21, 43-47; Reply Br. 6-7, 9-10, 13, 22-23.

"[W]aiver is the intentional relinquishment or abandonment of a known right." *U.S.*

¹⁰ The panel overstates the government's position. It relies on a single conclusory sentence of the government's brief, which states: "*To the extent* that the plaintiffs have preserved separate arguments about IP addresses, those arguments fare no better." Gov't Br. 19 (emphasis added). The brief invited no response.

v. Olano, 507 U.S. 725, 733 (1993) (internal quotation marks omitted); *Wainwright v. Sykes*, 433 U.S. 72, 83 (1977). All of the evidence indicates that the petitioners did not intend to waive their attachment of the IP addresses and therefore did not. *In re Sealed Case*, 121 F.3d at 740-41.

IV. Petitioners did not forfeit the enforcement of their writs

The panel found that petitioners forfeited TRIA § 201 and 28 U.S.C. 1610(a)(7) for failing to raise § 1610(a)(7) in their opening brief to this Court and failing to raise § 201 below. Op. 25-26. Neither contention has any relevance at all for two reasons:

1. Generally, a movant for affirmative dispositive relief must demonstrate entitlement to that relief; failure to do so generally requires denial of the motion. ICANN is the movant for affirmative relief, having sought to quash petitioners' writs of attachment. The panel nonetheless shifted the burden to petitioners, relying on a Seventh Circuit case that (it claims) holds sovereign attachment immunity to be a "default presumption" that the judgment creditor must defeat at the outset." Op. 20-21 (quoting *Rubin v. Islamic Rep. of Iran*, 637 F.3d 783, 800 (7th Cir. 2011)). But *Rubin* did not so hold; it held, rather, that the *district court* must find an exception to attachment immunity, regardless of whatever the parties do. *Rubin*, 637 F.3d at 800. The panel also relies on *Peterson v. Islamic Rep. of Iran*, 627 F.3d 1117, 1125 (9th Cir. 2010), which likewise supports petitioners' position. *Peterson* holds that upon the defendant's *prima facie* demonstration of entitlement to immunity, the plaintiffs have a "burden of production" and must produce "*evidence*" of entitlement to an exception to immunity. *Id.* (emphasis added). That obviously implies that the plaintiff may

attempt to obtain evidence through discovery. Here, the district court made no findings regarding attachment immunity (contrary to *Rubin*) and the petitioners have had materially no discovery and thus have never had a chance to satisfy their burden of production (violating *Peterson*). Because ICANN never met its burden as the movant for affirmative relief and petitioners never had a chance to counter ICANN's representations, the petitioners could not have possibly forfeited anything.

2. Petitioners' response to ICANN's motion to quash said virtually nothing on the merits. It argued that discovery is necessary before a meaningful response on the merits is possible. Petitioners reasonably expected that the district court would either grant their motion or else permit them to respond upon learning that there would be no discovery. The district court instead attempted to resolve this litigation without reaching questions that turned on factual issues requiring discovery, such as the immunity questions reached by this Court. It makes little sense to hold that, in that posture and notwithstanding that petitioners represented to the district court that they had a response on the merits but would delay making the argument until they could do so fully, the petitioners forfeited their arguments related to immunity. The crux of petitioners' representations to the district court was that the immunity issue was *unripe* for consideration. Failing to raise an argument before it is ripe is, by definition, not forfeiture, the "failure to make the timely assertion of a right." *Olano*, 507 U.S. 725, 733. Petitioners timely asserted their attachment and indicated that they would refute ICANN's arguments regarding immunity, but merely requested the tools to do so properly before traveling that path.

The district court did not refuse. Nor did it suggest anywhere that petitioners waived or forfeited any argument, notwithstanding that it could have easily quashed the writs of attachment on the basis of forfeiture. It opted instead to respect the petitioners' reasonable expectations and need for discovery; it rather focused on a discrete dispositive issue it found to be ripe. The panel should have afforded greater "respect" to the district court's "management of this...litigation" and its "efforts to impose order upon the issues in play" by honoring the district court's pre-discovery limitation of the issues. *Exxon Shipping v. Baker*, 554 U.S. 471, 487 n.6 (2008).

Following the lead of the district court, petitioners devoted their opening brief to the issues presented by the district court's opinion. Those issues did not include the statutory exceptions to attachment immunity, which is why petitioners did not discuss them. In its brief, ICANN raised attachment immunity despite that petitioners never had a "fair opportunity to dispute the facts material" to immunity. *Washburn v. Lavoie*, 437 F.3d 84, 89 (D.C. Cir. 2006). Even assuming that ICANN adequately placed those issues before the Court, the petitioners had the right to fully respond in their reply brief. *Van Smith*, 530 F.3d at 970 n.2; *Env'tl. Def. Fund*, 210 F.3d at 401 n.8. They did so and thereby avoided waiver and forfeiture.

CONCLUSION

For the reasons stated herein, this Court should grant rehearing, vacate the district court's decision, and remand for discovery.

Dated: August 31, 2016
Baltimore, Maryland

Respectfully submitted,

THE BERKMAN LAW OFFICE, LLC
Attorneys for Plaintiffs-Appellants

By: /s Meir Katz
Meir Katz

Robert Tolchin

Meir Katz

111 Livingston Street, Suite 1928

Brooklyn, New York 11201

718-855-3627

rtolchin@berkmanlaw.com

mkatz@berkmanlaw.com

Steven T. Gebelin

Scott M. Lesowitz

RAINES FELDMAN LLP

9720 Wilshire Boulevard, 5th Floor

Beverly Hills, California 90212

(310) 440-4100

sgebelin@raineslaw.com

slesowitz@raineslaw.com

ADDENDUM

United States Court of Appeals
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued January 21, 2016

Decided August 2, 2016

No. 14-7193

SUSAN WEINSTEIN, INDIVIDUALLY AS CO-ADMINISTRATOR OF
THE ESTATE OF IRA WILLIAM WEINSTEIN,
AND AS NATURAL GUARDIAN OF
PLAINTIFF DAVID WEINSTEIN (MINOR), ET AL.,
APPELLANTS

v.

ISLAMIC REPUBLIC OF IRAN, ET AL.,
APPELLEES

Consolidated with 14-7194, 14-7195, 14-7198,
14-7202, 14-7203, 14-7204

Appeals from the United States District Court
for the District of Columbia

(No. 1:00-cv-02601)

(No. 1:02-cv-01811)

(No. 1:08-cv-00520)

(No. 1:01-cv-01655)

(No. 1:08-cv-00502)

(No. 1:00-cv-02602)

(No. 1:14-mc-00648)

Meir Katz argued the cause for the appellants. *Robert J. Tolchin, Steven T. Gebelin* and *Scott M. Lesowitz* were with him on brief. *Jeffrey A. Miller* entered an appearance.

Noel J. Francisco argued the cause for the garnishee-appellee Internet Corporation for Assigned Names and Numbers. *Tara Lynn R. Zurawski* and *Ryan J. Watson* were with him on brief.

Benjamin C. Mizer, Principal Deputy Assistant Attorney General, United States Department of Justice, *Beth S. Brinkmann*, Deputy Assistant Attorney General, and *Douglas N. Letter, Mark R. Freeman* and *Sonia K. McNeil*, Attorneys, were on brief the for *amicus curiae* United States.

Before: GARLAND,* *Chief Judge*, HENDERSON, *Circuit Judge*, and RANDOLPH, *Senior Circuit Judge*.

Opinion for the Court filed by *Circuit Judge* HENDERSON.

KAREN LECRAFT HENDERSON, *Circuit Judge*: The plaintiffs—victims of terrorist attacks and their family members—hold substantial unsatisfied money judgments against defendants Islamic Republic of Iran (Iran), Democratic People’s Republic of Korea (North Korea) and Syrian Arab Republic (Syria) arising out of claims brought pursuant to the Foreign Sovereign Immunities Act (FSIA). To satisfy the judgments, the plaintiffs sought to attach Internet data managed by the Internet Corporation for Assigned Names and Numbers (ICANN) and, accordingly, served writs of attachment on ICANN. On ICANN’s motion, the district court quashed the writs, finding the data

* Chief Judge Garland was a member of the panel at the time the case was argued but did not participate in this opinion.

unattachable under District of Columbia (D.C.) law. We affirm the district court but on alternative grounds.

I. Background

A. TECHNICAL

This case requires substantial explanation of the sought-after data.¹ The plaintiffs initiated these proceedings by serving multiple writs of attachment on ICANN seeking the country-code top level domain names (ccTLD) and Internet Protocol (IP) addresses of Iran, Syria and North Korea, respectively. Neither the ccTLD nor the IP address lends itself to easy description.

Both data are parts of the Internet, the “network of networks,” *Am. Civil Liberties Union v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996), which is “comprised of numerous interconnected communications and computer networks connecting a wide range of end-users to each other.” *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir.

¹ In district court, the parties apparently agreed that the motion to quash should be decided under Federal Rule of Civil Procedure 12(b)(6). *See* Pls.’ Mot. for Six Month Discovery at 18 (describing ICANN’s motion and its timing as “akin to a defendant filing a Federal Rule 56 summary judgment motion at the very outset of a case”); ICANN’s Opp. to Pls’. Mot. for Six Month Discovery at 13 n.3 (responding that “Motion to Quash is functionally identical to a Rule 12(b)(6) motion to dismiss”). We resolve all factual disputes accordingly, “accepting as true all of the factual allegations contained in the [plaintiffs’ submissions] and drawing all inferences in favor of” the plaintiffs. *Autor v. Pritzker*, 740 F.3d 176, 179 (D.C. Cir. 2014) (alterations omitted).

2004).² The IP address is the appropriate starting point. Every device connected to the Internet and every web page on the Internet is identified by an IP address. The IP address appears as a string of numbers separated by periods, for example, “100.200.123.234.” It identifies the location, “*i.e.*, a particular computer-to-network connection” of an end-user’s computer and also “serves as the routing address for . . . requests to view a web page.” *Id.* The IP address is critical to the Internet’s functioning in the same way a telephone number is essential to the functioning of the telecommunications system. One may dial a set of numbers to connect to other individuals through the telecommunications system and the same is true vis-à-vis an IP address and the Internet. Granted, an ordinary Internet end-user does not operate this way. For example, Google has the IP address “173.194.65.113” but few would maintain that entering that address in an Internet browser is the most practical way to access the Google web page. Instead, most end-users simply type “google.com” to access the Google web page.

Because the numeric IP address is difficult to remember, the domain name system (DNS) was created to provide a more user-friendly Internet. At bottom, a “domain name” is the alphanumeric “Web page address[] that end users type into their browsers” and the DNS matches that name (*i.e.*, “google.com”) “with the [IP] addresses of the servers containing the Web pages the users wish to access.” *Nat’l Cable & Telecomm’n Ass’n v. Brand X Internet Servs.*, 545 U.S. 967, 987 (2005). Thus, much of the DNS’s value lies in its ability to enable an end-user, with a domain name in hand,

² We hereinafter use “end-user” to refer to an individual seeking to access a web page on the Internet through an Internet browser.

to access a desired IP address and, more importantly, its corresponding web page without in fact *using* the IP address. But unlike an IP address, “a domain name does not signal where a computer [or web page] is . . . located. . . . [A] domain name is not an address as typically understood but instead is a mark identifying a specific person’s or organization’s site on the Internet.” *Thomas v. Network Solutions, Inc.*, 176 F.3d 500, 503 n.2 (D.C. Cir. 1999). In order to reach the “site,” the user’s domain name input must be “translate[d] . . . into [a] numerical IP address,” *Register*, 356 F.3d at 410–11 & n.14, *i.e.*, the domain name must be “resolved,” *Name.Space, Inc. v. Network Solutions, Inc.*, 202 F.3d 573, 577 (2d Cir. 2000).

Understanding the “resolving” process begins with breaking down an Internet web page name—*i.e.* a domain name (“google.com”)—into two parts. The first part appears after the last dot—the “top level domain” (TLD). As relevant here, there are two types of TLDs: generic TLDs and country code TLDs (ccTLDs). The former include “.com,” “.net” and “.org” whereas the latter are distinguished by a national, geographic or political association—for example, “.us” for the United States and, here, “.ir” for Iran, “.sy” for Syria and “.kp” for North Korea.³ The second part precedes the last dot—the second level domain (SLD); *i.e.*, “google” in the “google.com” example.

Broadly speaking, an Internet end-user searching for (the technical term is “querying”) a domain name like

³ The plaintiffs also sought to attach the defendants’ internationalized TLDs—TLDs that appear in a country’s language-specific font—*i.e.*, “ناري.ا” for Iran. For simplicity, and because the parties do not treat them differently, we use the term “ccTLDs” to refer to both the conventional and the internationalized ccTLDs.

“google.com” reaches the web page in one of two ways depending on whether he already has visited that web page. In either case, his device ordinarily first sends the query to a nearby DNS “caching server” operated by the end-user’s Internet service provider (ISP).⁴ See Daniel Karrenberg, *The Internet Domain Name System Explained for Non-Experts*, in INTERNET GOVERNANCE: A GRAND COLLABORATION 23 (U.N. ICT Task Force 2004). The caching server knows the location of the web page if it has “cached” it, *i.e.*, “remembered it . . . from a previous transaction.” *Id.* at 24. In that case the query does not go beyond the caching server because it directs the end-user to the desired location. *Id.* Thus, once an end-user has visited “google.com,” his caching server remembers the web page location for subsequent visits. And if the end-user has never visited the requested SLD—*i.e.*, never visited “google.com”—but has visited another “.com” web page (*e.g.*, “amazon.com”), the caching server recognizes the location of the TLD (“.com”), asks it for the location of the SLD (“google.com”) and then routes the end-user accordingly. *Id.* at 26–27.

An end-user can also locate a web page if he has not yet visited the web page or even its TLD. This way involves a caching server that is empty—it does not know the location of “.com,” and even less “google.com,” because it has not yet cached them. But the caching server knows at least *one* thing: Pursuant to widely adopted pre-programmed DNS protocols, the server knows to query “a special set of authoritative

⁴ As its name suggests, an ISP is “an entity that provides access to the Internet.” *Register*, 356 F.3d at 410 n.13. Every individual “Web [page], company, university, and government agency that utilizes Internet access . . . subscribes to an ISP or is one.” *Id.* at 410 n.13. Commonly-used ISPs include Comcast and Verizon.

servers” otherwise known as “the DNS root servers,” *id.* at 27—of which there are thirteen world-wide; namely, one “master root zone server,” which contains “the authoritative root zone file,”⁵ and “12 duplicate root zone servers,” *Name.Space*, 202 F.3d at 577. In short, the caching server knows to go to the top of the DNS’s “hierarchical tree structure.” *Id.* These thirteen servers—the top of the tree—know the location of all authoritative TLD servers and thus the caching server can locate “.com,” “.ir” or any other TLD by querying the DNS root servers. Once one of the root servers tells the caching server the “.com” location, the caching server can query that TLD for all SLDs within it and does not have to revisit the root servers for subsequent web page searches within the “.com” TLD.⁶ Thus the root servers form “a critical Internet chokepoint.” A. Michael Froomkin, *Wrong Turn in Cyberspace*, 50 DUKE L.J. 17, 50 (2000). To use the entire DNS, a caching server need know nothing more than the location of the DNS’s thirteen root servers; the root servers, tied to the root zone file, permit any end-user to access all downstream domains.

As relevant here, the DNS’s “hierarchical tree structure,” *Name.Space*, 202 F.3d at 577, contains three levels—the thirteen root zone servers at the top, TLDs one level below and SLDs one level further below. Each level of the tree “registers” entities one level below. *See* Harold Feld,

⁵ The root zone file is a file that “contains information on the TLDs within the [DNS] and the location of . . . those TLDs.” *Stern*, 73 F. Supp. 3d 46, 49 (D.D.C. 2014). According to the DNS, the thirteen root servers are “authoritative” because they reflect the information contained in the root zone file.

⁶ Nevertheless, in reality, a caching server regularly discards its cached information and revisits the root servers to ensure it has current information.

Structured to Fail: ICANN and the 'Privatization' Experiment, in WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION 337–38 (Cato Inst. 2003). Thus, a TLD must be registered in the root servers' root zone file in order to be accessible to an end-user. The relationship between SLDs and TLDs is similar. An SLD registers within a TLD; thus, one can access Google only by searching for it in a TLD that it is registered within, *i.e.*, the “.com” TLD. And, just as a particular TLD ensures that no duplicate domain name is registered within (*i.e.*, the “.com” registry allows only one “google.com”), the root zone file ensures that there is only one of each TLD (*i.e.*, only one “.com”). When searched, that is the TLD to which the DNS root server directs an end-user. Because “the vast majority of Internet users,” via their ISP, query the root servers when searching for a particular TLD, “[t]he root [zone file] determines which TLDs are visible” to most Internet end-users world-wide. *Wrong Turn in Cyberspace*, 50 DUKE L.J. at 46. Because an end-user cannot use the DNS to locate a particular web page without first accessing its TLD—*i.e.*, an end-user cannot locate “google.com” without first locating “.com”—the root zone file effectively enables an end-user to access most existing Internet web pages. Any TLD not “listed in the root . . . become[s] effectively invisible,” *id.* at 47, keeping both that TLD and its registered SLDs beyond the reach of a typical end-user.

With the DNS background established, we turn to ICANN. From shortly after its inception in 1983 until 1998, the root zone file and the DNS were administered by “private hands” under “loose federal supervision.” Harold Feld, *Structured to Fail: ICANN and the 'Privatization' Experiment, in WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION* 335 (Cato Inst. 2003). In 1998 the United States government transferred much of its

oversight role to ICANN, a California non-profit corporation. ICANN's mission is to "protect the stability, integrity, interoperability and utility of the DNS on behalf of the global Internet community," Decl. of John O. Jeffrey, App'x 24.2 ¶ 5, and, pursuant to a contract with the United States Department of Commerce (Commerce Department), the organization now performs several functions essential to the functioning of the Internet.

Each TLD requires management. ICANN's first responsibility relevant to this case is its selection and approval of qualified entities to operate each of the Internet's TLDs—"registry operators" in ICANN parlance. Regarding the ccTLDs, ICANN uses a comprehensive procedure for those seeking delegation or re-delegation of registry responsibilities (*i.e.*, ccTLD management). Among other things, a proposed ccTLD manager must (1) possess administrative and technical competency, (2) ordinarily be located in the applicable country or territory, (3) obtain consent from affected parties, (4) manifest its commitment to serve the local Internet community's interest and (5) demonstrate that the appropriate local government does not object to the delegation or re-delegation.⁷

Obtaining ICANN approval for ccTLD management, however, does not automatically effect a registry change. The delegation or re-delegation is effective only if recorded in the root zone file. But ICANN cannot make changes to the root

⁷ Pursuant to ICANN publications, it is "expected that relevant local governments are consulted" but it is "not a requirement that they consent." See *Common Questions on Delegating and Redelegating Country-Code Top-Level Domains (ccTLDs)*, IANA.ORG, <https://www.iana.org/help/cctld-delegation-answers> (last visited July 7, 2016).

zone file. Rather, Verisign, another American company, performs the recording function under contract with the Commerce Department. The Commerce Department approves all ICANN ccTLD management delegations and re-delegations and instructs Verisign to implement the corresponding root zone file change. Thus, ICANN screens and recommends, the Commerce Department authorizes and Verisign implements all changes to ccTLD management.⁸

ICANN's second relevant function is the distribution of IP addresses. First, ICANN generates and distributes IP addresses to regional Internet registries (RIRs). There are five RIRs world-wide, each responsible for its own multi-country geographic zone. The RIRs then distribute the IP addresses further downstream; ultimately to end-users and web page operators. Once a website operator obtains an IP address, its web page becomes Internet-accessible. In the usual course, the operator then acquires and links a domain name to the web page in order to use the DNS.

B. PROCEDURAL

The plaintiffs, victims of terrorist attacks as well as surviving family members of those killed in the attacks, have obtained judgments amounting to hundreds of millions of dollars against the defendant governments for their respective roles in those attacks. *See Weinstein v. Islamic Republic of Iran*, 184 F. Supp. 2d 13 (D.D.C. 2002) (\$ 183,248,164 in compensatory and punitive damages); *Haim v. Islamic*

⁸ *But see* Br. for United States as *Amicus Curiae* at 6 (describing government role as “largely symbolic” in that it is “limited to ensuring that ICANN has followed appropriate processes and avoided technical errors”); *see also id.* (“The policy of the United States is that the Internet’s [DNS] should be free from the control of any government, including our own.”).

Republic of Iran, 425 F. Supp. 2d 56 (D.D.C. 2006) (*Haim I*) (\$ 16,000,000 in compensatory damages); *Haim v. Islamic Republic of Iran*, 784 F. Supp. 2d 1 (D.D.C. 2011) (*Haim II*) (\$ 300,000,000 in punitive damages); *Campuzano v. Islamic Republic of Iran*, 281 F. Supp. 2d 258 (D.D.C. 2003) (\$ 259,000,000 in compensatory and punitive damages to Rubin plaintiffs); *Wyatt v. Syrian Arab Republic*, 908 F. Supp. 2d 216 (D.D.C. 2012) (\$ 338,000,000 in compensatory and punitive damages); *Stern v. Islamic Republic of Iran*, 271 F. Supp. 2d 286 (D.D.C. 2003) (\$ 313,000,000 in compensatory and punitive damages); *Calderon-Cardona v. Democratic People's Republic of Korea*, 723 F. Supp. 2d 441 (D.P.R. 2010) (\$ 378,000,000 in compensatory and punitive damages). For example, in *Weinstein* the plaintiffs, proceeding under the FSIA's "state sponsor of terrorism" exception to immunity from suit, *see* 28 U.S.C. § 1605(a)(7),⁹ alleged that Iran sponsored the organization—HAMAS—which detonated a bomb that killed the plaintiffs' kin. A default judgment was awarded pursuant to the state-sponsored terrorism exception and 28 U.S.C. § 1608 ("No judgment by default shall be entered . . . unless the claimant establishes his claim or right to relief by evidence satisfactory to the court."). This suit is the latest—although not the only¹⁰—attempt to recover on the various judgments.

On June 24, 2014 the plaintiffs served writs of attachment on ICANN seeking the defendants' ccTLDs and

⁹ This provision has been updated and re-codified at 28 U.S.C. § 1605A, *see infra* nn.21, 22.

¹⁰ *See, e.g., Calderon-Cardona v. Bank of New York Mellon*, 770 F.3d 993 (2d Cir. 2014) (failed attempt to attach North Korean electronic funds transfers in American banks); *Rubin v. Islamic Republic of Iran*, 709 F.3d 49 (1st Cir. 2013) (failed attempt to attach alleged Iranian antiquities in American museums).

“supporting IP addresses” and subpoenas *duces tecum* seeking information regarding those data. Decl. of Eric P. Enson, Supp. App’x 45–46. ICANN then moved to quash the writs, arguing that (1) the data are not “property” subject to attachment; (2) the defendants do not own the data; (3) the data are not located within D.C. or even the United States; (4) ICANN lacks unilateral authority to transfer/re-delegate the data and (5) the court lacked jurisdiction to issue the writs.¹¹ After two months of discovery, the plaintiffs sought a six-month extension arguing that ICANN had produced limited information and that further discovery was needed regarding, as relevant here, ICANN’s contention that ccTLDs and IP addresses are not “property.” In support thereof, the plaintiffs submitted the declaration of one of their counsel who memorialized a discussion he had conducted with an expert on Internet infrastructure and DNS operators. According to the declarant, ICANN “ha[s] a monopoly or complete control over the ‘root zone’ such that ICANN is wholly and solely responsible for the mapping of [ccTLDs] to their respective registries/name servers.” Decl. of Steven T. Gebelin at 3, App’x 51 (Gebelin Decl.). Also according to the declarant, the alleged expert explained that ICANN had in the past “changed and redirected who runs certain ccTLDs . . . in

¹¹ ICANN initially argued that the writs themselves were invalid because they were not court-issued. *See* ICANN’s Objections and Verified Answers to Writ of Attachment Interrogatories at 3, Dkt. No. 88 (“ICANN objects to the Writ of Attachment and each and every Interrogatory on the grounds, and in that, they were not properly executed by the Court, as is required by the Foreign Sovereign Immunities Act.”). *See* 28 U.S.C. § 1610(c) (“no attachment or execution . . . shall be permitted until the court has ordered such attachment and execution after having determined that a reasonable period of time has elapsed following the entry of judgment”). The district court did not address the argument and ICANN has not pursued it on appeal.

conjunction with the ‘monetization’ of the ccTLDs by their respective governments, including instances where the governments transferred control away from academic communities to government approved third parties that acquired contractual property rights to exploit the ccTLD and generate revenue.” *Id.* In short, the alleged expert opined that ccTLDs are property that a sovereign can own and monetize and that ICANN has unbridled authority to redelegate them.

The district court granted ICANN’s motion to quash on November 10, 2014. Applying local law pursuant to FED. R. CIV. P. 69(a)(1) (“[P]rocedure on execution—and in proceedings supplementary to and in aid of judgment or execution—must accord with the procedure of the state where the court is located, but a federal statute governs to the extent it applies.”), the court held that ccTLDs are not “goods, chattels [or] credits” within the meaning of D.C. Code § 16-544,¹² *Stern*, 73 F. Supp. 3d at 50–51; accordingly, the court concluded that “there [we]re no factual disputes that require further consideration” and denied as moot the plaintiffs’ motion for extended discovery. *Id.* at 51 n.3. On appeal the plaintiffs challenge the district court’s interpretation of D.C. law and suggest certification to the D.C. Court of Appeals pursuant to D.C. Code § 11–723(a) (“The District of Columbia Court of Appeals may answer questions of law certified to it by . . . a Court of Appeals of the United States.”). They also claim that the district court abused its discretion in denying further discovery. Our jurisdiction is based on 28 U.S.C. § 1291.

¹² D.C. Code § 16–544 provides that “[a]n attachment may be levied upon the judgment debtor’s goods, chattels, and credits.”

II. Analysis

A. ATTACHMENT IMMUNITY UNDER FSIA § 1609

The FSIA provides “a comprehensive set of legal standards governing claims of immunity in every civil action against a foreign state,” *Verlinden B.V. v. Cent. Bank of Nigeria*, 461 U.S. 480, 488 (1983), as well as the “sole basis for obtaining jurisdiction over a foreign state in our courts,” *Argentine Republic v. Amerada Hess Shipping Corp.*, 488 U.S. 428, 434 (1989). The statute establishes “two kinds of immunity” for a foreign sovereign. *Republic of Argentina v. NML Capital, Ltd.*, 134 S. Ct. 2250, 2256 (2014). First, as a matter of “subject matter jurisdiction,” *Verlinden*, 461 U.S. at 489, the FSIA establishes immunity from *suit* in “the courts of the United States and of the States,” 28 U.S.C. § 1604. The seven judgments obtained were awarded pursuant to the state-sponsored terrorism exception to the defendant sovereigns’ immunity from suit, 28 U.S.C. § 1605A. *See supra* at 10–11.¹³ Second, it establishes immunity from “attachment[,]

¹³ The judgments in *Haim I*, *Weinstein* and *Stern* were entered under the former state-sponsored terrorism exception, 28 U.S.C. § 1605(a)(7), but those plaintiffs did not convert their judgments to the exception’s current version, 28 U.S.C. § 1605A. The plaintiffs concede this point and do not argue for its application to their respective judgments. *See* Appellants’ Reply Br. at 23–24 (asserting only *Haim II*, *Rubin*, *Wyatt and Calderon-Cardona* judgments were entered or converted under section 1605A); *see also* Appellee’s Br. at 50 (*Haim I*, *Weinstein* and *Stern* “were neither entered nor converted to a judgment under § 1605A.”). A judgment entered under former 1605(a)(7) does not—without conversion—trigger section 1610(g). *See infra* at 21–24.

arrest and execution,” 28 U.S.C. § 1609.¹⁴

ICANN contends that, because the plaintiffs did not adequately establish an exception to attachment immunity under the FSIA, 28 U.S.C. §§ 1609–1611, the district court lacked subject matter jurisdiction to “execute against” the defendant sovereigns’ property. Appellee’s Br. at 39–40. ICANN is mistaken, however, about the jurisdictional nature of attachment immunity. Although the Supreme Court has never expressly addressed whether attachment immunity is jurisdictional, it has in dicta suggested otherwise. *See Akins v. FEC*, 66 F.3d 348, 354 (D.C. Cir. 1995) (“Supreme Court[] dicta . . . not bind[ing]” but “reliance on dicta may nonetheless be reasonable”); *see also ACLU of Ky. v. McCreary Cnty., Ky.*, 607 F.3d 439, 447 (6th Cir. 2010) (inferior court generally “obligated to follow Supreme Court dicta” absent “substantial reason for disregarding it”). In *NML Capital*, the Court referred to the first “kind of immunity” as “jurisdictional immunity” and the latter as both the “immunity defense” and “execution immunity.” 134 S. Ct. at 2256. We are without “substantial reason for disregarding” this distinction, *see ACLU of Ky.*, 607 F.3d at 447, and the majority of our sister circuits that have considered the issue are in accord, *see Peterson v. Islamic Republic of Iran*, 627 F.3d 1117, 1125 (9th Cir. 2010) (“[S]overeign immunity from execution does not defeat a court’s jurisdiction”); *Rubin v. Islamic Republic of Iran*, 637 F.3d 783, 800 (7th Cir. 2011) (same).¹⁵ We follow suit and

¹⁴ 28 U.S.C. § 1609 provides in relevant part that “the property in the United States of a foreign state shall be immune from attachment arrest and execution except as provided in sections 1610 and 1611”

¹⁵ One circuit has reached a contrary result, *see FG Hemisphere Assocs. v. Republique du Congo*, 455 F.3d 575, 590–

reject ICANN's challenge to the district court's subject matter jurisdiction.

B. FEDERAL RULE OF CIVIL PROCEDURE 69(a) AND D.C.
CODE § 16-544

Applying the reasoning of the Virginia Supreme Court in *Network Solutions, Inc. v. Umbro Int'l, Inc.*, 259 Va. 759 (2000), the district court observed;

[t]he ccTLDs exist only as they are made operational by the ccTLD managers that administer the registries of second level domain names within them and by the parties that cause the ccTLDs to be listed on the root zone file. A ccTLD, like a domain name,

91 (5th Cir. 2006), but did so relying, in our view, on inapposite precedent. The *FG Hemisphere* court cited a trio of Supreme Court FSIA cases to inform its analysis of section 1609 but they addressed only the Act's immunity from suit provision, 28 U.S.C. § 1604. Granted the Fifth Circuit also cited *Schooner Exchange v. McFaddon*, 11 U.S. 116 (1812), for the proposition that "American courts ha[ve] no *jurisdiction* over" a foreign sovereign's property, *FG Hemisphere*, 455 F.3d at 590 (emphasis added). In *Schooner Exchange* the Court held that certain property of France was "exempt from the jurisdiction of" our courts, *Schooner Exch.*, 11 U.S. at 147, and the case is "generally viewed as the source of our foreign sovereign immunity jurisprudence," *Republic of Austria v. Altmann*, 541 U.S. 677, 688 (2004). It is inapposite here, however, because it involved an attempt to exercise *in rem* jurisdiction despite the plaintiff's not having obtained a valid judgment against France. *Schooner Exch.*, 11 U.S. at 117. FSIA sections 1609–1611—those governing attachment—operate only after the award of a valid judgment. See H.R. Rep. 94-1487 at 26 (1976), reprinted in 1976 U.S.C.C.A.N. 6604, 6625 ("[S]ection 1609 has the effect of precluding attachment as a means for commencing a lawsuit.").

cannot be conceptualized apart from the services provided by these parties. The Court cannot order plaintiffs' insertion into this arrangement.

Stern, 73 F. Supp. 3d at 50 (internal quotations omitted). It then relied on the D.C. Court of Appeals' holding in *Cummings General Tire Co v. Volpe Construction Co.*, 230 A.2d 712, D.C. 1967), to conclude that the ccTLDs "may not be attached in satisfaction of the plaintiffs' judgments because they are not properly subject to attachment under District of Columbia law." *Stern*, 73 F. Supp. 3d at 51.¹⁶ Accordingly, the district court quashed the writs of attachment under local law, interpreting FED. R. CIV. P. 69(a) to require its application. *See Stern*, 73 F. Supp. 3d at 49–50.¹⁷

Similarly, ICANN uses the Rule 69(a) portal to argue, *inter alia*, that ccTLDs are not "goods, chattels, [or] credits" within the meaning of D.C. Code § 16–544 (permitting attachment "upon the judgment debtor's goods, chattels, and credits") and that local law prohibits attachment both because the data are "inextricably bound up with the provision of services" and because ICANN "cannot transfer them unilaterally or even at Defendants' behest." Appellee's Br. at 14–32. We assume without deciding that local law applies to the determination of the "attachability" of the defendant sovereigns' ccTLDs.¹⁸ In addition, we assume without so

¹⁶ As explained *infra* at 26–27, the district court did not address the IP addresses.

¹⁷ The district court denied the plaintiffs' discovery motion as moot. *See id.* at 51 n.3. We affirm for the same reason.

¹⁸ Although we assume the applicability of D.C. Code § 16–544, we nonetheless have reservations about its applicability. Federal Rule of Civil Procedure 69(a)(1) ("The procedure on

execution—and in proceedings supplementary to and in aid of judgment or execution—must accord with the procedure of the state where the court is located, but a federal statute governs to the extent it applies.”) contains significant limiting language. It incorporates only local *procedure*. There are precious few *federal* rules of procedure for execution of judgments; the draftsmen evidently “decided . . . to borrow the format employed in the courts of the forum state,” *Resolution Trust Corp. v. Ruggiero*, 994 F.2d 1221, 1226 (7th Cir. 1993), at least in part to enable a plaintiff to *execute* on a federal judgment, *see, e.g., United States v. Harkins Builders, Inc.*, 45 F.3d 830, 833 (4th Cir. 1995) (“Even though we look to state law to determine the . . . procedure to be followed . . . we do so in furtherance of federal law, giving effect to rules entitling parties to enforce federal judgments in federal courts.”); *cf. Peacock v. Thomas*, 516 U.S. 349, 359 (1996) (“[T]he Federal Rules of Civil Procedure provide fast and effective mechanisms for execution” in order “[t]o *protect* and *aid* the collection of a federal judgment.” (emphases added)).

In our view, application of Rule 69(a)(1) requires a preliminary determination, *i.e.*, whether D.C. Code § 16–544 is in fact procedural. The answer may depend on an inquiry materially identical to the Supreme Court’s so-called reverse-*Erie* precedent holding that the “general and unassailable proposition” that local “rules of procedure govern[] litigation” can be overcome if their application is “outcome-determinative.” *Felder v. Casey*, 487 U.S. 131, 138, 141 (1988). The “reverse-*Erie*” title is plainly a nod to the inquiry undertaken when a federal court hearing a *state* law claim must decide whether an issue is “substantive”—and thus determined by state law—or “procedural” and thus subject to the federal rules. *See Hanna v. Plumer*, 380 U.S. 460, 465 (1965); *see also Gasperini v. Ctr. for Humanities, Inc.*, 518 U.S. 415, 428 (1996) (applying *Erie*’s “outcome-determinati[ve] test” with reference to “the twin aims of the *Erie* rule: discouragement of forum-shopping and avoidance of inequitable administration of the laws” (internal quotation marks omitted)). Here the proceedings involve a federal, not state, claim. This difference has little significance given Rule 69’s broad directive to apply the procedure

holding that local law does not operate to bar attachment of the defendant sovereigns' ccTLDs.¹⁹

“of the state where the court is located.” FED. R. CIV. P. 69(a)(1). But if, per reverse-*Erie*, a procedure is inapplicable in state court, it would not “accord with the procedure of the state” for the *federal* court to use that procedure. *Id.*

Granted, in dated cases regarding the scope of “Revised Statutes § 916” (RS 916)—a Rule 69 predecessor, *see United States v. Yazell*, 382 U.S. 341, 355 (1966), the Supreme Court in effect held that the Congress “adopted” all state laws bearing on execution, *Fink v. Oneil*, 106 U.S. 272, 277 (1882). But RS 916 and Rule 69 contain materially different language, making *Fink* inapposite. In addition, modern cases confirm that the *Fink* Court’s wholesale adoption of state execution law is, like RS 916, a relic. In *Mackey v. Lanier Collection Agency & Serv., Inc.*, 486 U.S. 825 (1988), faced with the assertion that a Georgia “state procedural device for collecting judgments”—garnishment—was in fact “substantive,” the Court examined its features before confirming its procedural nature and resulting applicability via Rule 69. *Id.* at 834 n.10 (“under Georgia law, postjudgment garnishment is nothing more than a method to *collect* judgments *otherwise* obtained” (second emphasis in original)).

¹⁹ Assuming, again without deciding, that Rule 69(a)(1) can be interpreted to incorporate a local law attachment bar, execution on a *FSIA* judgment requires caution for another reason. “[A]ctions against foreign sovereigns in our courts raise sensitive issues concerning the foreign relations of the United States.” *Verlinden*, 461 U.S. at 493. Moreover, the conduct of our nation’s foreign affairs, if not “vested in the national government exclusively,” *United States v. Pink*, 315 U.S. 203, 233 (1942), nonetheless restricts “[a]ny concurrent state power . . . to the narrowest of limits,” *Hines v. Davidowitz*, 312 U.S. 52, 68 (1941). If a state court’s application of a bar on property alienation vis-à-vis a foreign sovereign represents an unconstitutional “intrusion by the State into the field of foreign affairs,” *Zschernig v. Miller*, 389 U.S.

C. FSIA'S EXEMPTIONS TO EXECUTION IMMUNITY

Although attachment immunity is not “jurisdictional,” it is nonetheless a “default presumption” that the judgment

429, 430, 432 (1968) (concluding Oregon law providing property of deceased resident escheats if government of nonresident alien heirs prohibited inheritance without interference unconstitutionally intruded on foreign affairs), it can be argued that a federal court’s similar application via Rule 69(a) would not “accord with the procedure of the state,” FED. R. CIV. P. 69(a), at least, not with a procedure that is—in this arena—constitutional.

The Supreme Court has consistently set aside state laws that materially impede the national government’s conduct of foreign affairs, including disposition of foreign assets. In *United States v. Belmont*, the federal government sought to recover property in federal district court from a banker with whom a Russian corporation had deposited funds before the U.S.S.R.’s nationalization of all “property and assets of every kind and wherever situated, including the deposit account” in dispute. 301 U.S. 324, 326 (1937). The United States rested its claim on an “international compact” with the Soviet government wherein the latter “released and assigned to [the United States] . . . the deposit account.” *Id.* at 326, 327. The district court held that, because the “bank deposit was within the state of New York . . . in no sense could it be regarded as an intangible property right within the Soviet territory” and thus a “judgment for the United States . . . would be contrary to the controlling public policy of the state of New York.” *Id.* at 327. The Supreme Court did not “pause to inquire whether in fact there was any policy of the state of New York to be infringed” because, in foreign affairs, “state lines disappear. . . [and] the state of New York *does not exist.*” *Id.* at 327, 331 (emphasis added). Calling it “inconceivable” for any “[s]tate Constitutions, state laws, and state policies” to “be interposed as an obstacle to the effective operation of” the federal power, the Court reversed. *Id.* at 332; *see also Pink*, 315 U.S. at 231–33.

creditor must defeat at the outset. *See Rubin*, 637 F.3d at 800; *see also Peterson*, 627 F.3d at 1125 (execution immunity begins with “presumption that a foreign state is immune and then the plaintiff must prove that an exception to immunity applies”); *see also* 28 U.S.C. § 1609 (defendant sovereign’s property “shall be immune . . . *except* as provided in sections 1610 and 1611” (emphases added)). In particular, the plaintiffs *now*²⁰ rely on one or more of three exceptions. The first is the terrorist activity exception, which provides in relevant part that

[T]he property of a foreign state against which a judgment is entered under section 1605A,²¹ and the property of an agency or instrumentality of such a state, including property that is a separate juridical entity or is an interest held directly or indirectly in a separate juridical entity, is subject to attachment in aid of execution, and execution, upon that judgment as provided in this section, regardless of—

²⁰ ICANN contends that the plaintiffs forfeited or waived reliance on *any* exception to attachment immunity by failing either to raise the issue adequately in district court or to brief it on appeal. *See infra* at 25–26.

²¹ Section 1605A is the state-sponsored terrorism exception to a foreign sovereign’s general jurisdictional immunity. It abrogates suit immunity if “money damages are sought against a foreign state for personal injury or death that was caused by an act of torture, extrajudicial killing, aircraft sabotage, hostage taking, or the provision of material support or resources for such act.” 28 U.S.C. § 1605A(a)(1). Courts “shall” hear claims brought under this section if “the foreign state was designated as a state sponsor of terrorism at the time the [aforementioned terrorist act] occurred, or was so designated as a result of such act.” *Id.* § 1605A(a)(2)(A).

(A) the level of economic control over the property by the government of the foreign state;

(B) whether the profits of the property go to that government;

(C) the degree to which officials of that government manage the property or otherwise control its daily affairs;

(D) whether that government is the sole beneficiary in interest of the property; or

(E) whether establishing the property as a separate entity would entitle the foreign state to benefits in United States courts while avoiding its obligations.

28 U.S.C. § 1610(g). The second is the commercial activity exception, which provides in relevant part that

The property in the United States of a foreign state . . . used for a commercial activity in the United States, shall not be immune from attachment in aid of execution, or from execution, upon a judgment entered by a court of the United States or of a State . . . if the judgment relates to a claim for which the foreign state is not immune under section 1605A or section 1605(a)(7) (as such section was in effect on January 27, 2008),²² regardless of whether the property is or was

²² Section 1605(a)(7), as it read on January 27, 2008, is materially identical to current section 1605A.

23

involved with the act upon which the claim is based.

28 U.S.C. § 1610(a)(7). And the third exception the plaintiffs press to us is section § 201 of the Terrorism Risk Insurance Act (TRIA), which provides in relevant part that

[I]n every case in which a person has obtained a judgment against a terrorist party on a claim based upon an act of terrorism, or for which a terrorist party is not immune under section 1605A of [the FSIA] . . . , the blocked assets of that terrorist party . . . shall be subject to execution or attachment in aid of execution in order to satisfy such judgment to the extent of any compensatory damages for which such terrorist party has been adjudged liable.

28 U.S.C. § 1610 note.

To preserve an argument on appeal a party must raise it both in district court and before us. *Odhiambo v. Republic of Kenya*, 764 F.3d 31, 35 (D.C. Cir. 2014) (“[Plaintiff] does not renew [his FSIA exception] argument on appeal, so we do not consider it.”). The party must brief the issue with specificity. *See Railway Labor Executives’ Ass’n v. U.S. R.R. Retirement Bd.*, 749 F.2d 856, 859 n.6 (D.C. Cir. 1984).

Regarding the terrorist activity exception, the plaintiffs made minimal reference thereto both in district court and in their opening appellate brief. In its motion opposing extended discovery, ICANN argued that “the FSIA divests this Court of subject matter jurisdiction,” ICANN’s Opp. to Pls.’ Mot. for Six-Month Discovery at 8, to which the plaintiffs responded, *inter alia*, that “Section 1610(g) [removes immunity from] property of a foreign state against which judgment is entered

under 1605A,” and that “ICANN completely ignores Section 1610(g).” Reply in Supp. of Pls.’ Mot. for Discovery 19 & n.13. On appeal the plaintiffs noted that we have “federal question jurisdiction” under “28 U.S.C. § 1610” and included as an addendum the text of section 1610(g). Appellants’ Br. at 1, a3.

Ordinarily we might find these “fleeting statement[s]” insufficiently developed to preserve the argument, *see Am. Wildlands v. Kempthorne*, 530 F.3d 991, 1001 (D.C. Cir. 2008), but the terrorist activity exception is, simply put, different. Once a section 1605A judgment is obtained, section 1610(g) strips execution immunity from *all* property of a defendant sovereign. There is no genuine dispute that four of the plaintiffs’ judgments were entered or converted under 1605A.²³ Granted, the plaintiffs must show that the assets in question are “property of” the foreign sovereign, 28 U.S.C. § 1610(g), whether Iran, North Korea or Syria. In our view, there is no additional “argument” that must be preserved. *See Odhiambo*, 764 F.3d at 35. To the extent the plaintiffs must establish that the data at issue are “property” that each defendant has at least *some* ownership interest in, those matters were the subject of additional discovery requests (ultimately deemed moot by the district court) and so it would be premature for us to decide that their attachability is forfeited on that basis. On appeal the plaintiffs included the exception in their opening brief addendum and this was sufficient to put both us and ICANN on notice that they continued to rely on that exception.

²³ *See, e.g., Rubin v. Islamic Republic of Iran*, 563 F. Supp. 2d 38, 39 n.3 (D.D.C. 2008) (giving effect to plaintiff’s judgment “as if the action had originally been filed under section 1605A(c).”). *Cf. supra* n.13. *Accord Heiser*, 735 F.3d at 937 n.4.

Four of the seven underlying judgments, *Haim II*, 784 F. Supp. 2d 1 (D.D.C. 2011); *Campuzano v. Islamic Republic of Iran*, 281 F. Supp. 2d 258 (D.D.C. 2003) (*Rubin*); *Wyatt v. Syrian Arab Republic*, 908 F. Supp. 2d 216 (D.D.C. 2012); *Calderon-Cardona v. Democratic People's Republic of Korea*, 723 F. Supp. 2d 441 (D.P.R. 2010), were entered under section 1605A. ICANN, however, argues that “the plaintiffs presented no explanation or evidence” regarding these judgments. Appellee Br. at 49 (quotation marks omitted). We are at a loss to discern what “evidence” the plaintiffs would be required to show under ICANN’s approach, particularly given that ICANN does not appear to dispute that four judgments were entered under section 1605A. *Id.* at 50 (“[The terrorist activity exception] is clearly inapplicable to three of the seven underlying judgments at issue here.”). Therefore, the plaintiffs have not forfeited reliance on the terrorist activity exception to attachment immunity regarding the *Haim II*, *Wyatt*, *Rubin* and *Calderon-Cardona* judgments.

The two remaining exceptions are easily disposed of.²⁴ There is no reference to the commercial activity exception in the plaintiffs’ opening brief notwithstanding ICANN vigorously contested in district court whether the three ccTLDs were “used for a commercial activity in the United States.” 28 U.S.C. § 1610(a); *see* ICANN’s Mot. to Quash at 18 (“ICANN is aware of no evidence that the [] ccTLDs are used for commercial activity of the defendants in the United States.”). The plaintiffs rebutted this assertion in district court, *see* Reply in Supp. of Pls.’ Mot. for Discovery at 19 (“[T]he Internet Assets at issue are used for commercial

²⁴ The commercial activity exception covers all seven judgments and the TRIA exception applies only to the judgments obtained in *Weinstein*, *Haim I* and *Stern*.

activity in the United States and the United States is the situs. For example, a .ir second level domain can be purchased in the United States for approximately \$100.”), but on appeal they failed even to reference their objection in their opening brief. *See* Appellants’ Br. at 1–2 (“[I]ssues presented” includes only whether the assets are attachable property under D.C. law, whether the district court erroneously failed to allow additional discovery and whether we should pursue certification to the D.C. Court of Appeals). Their failure to brief the issues in their opening brief amounts to forfeiture. *Odhiambo*, 764 F.3d at 35. Their reliance on the TRIA exception likewise merits no close analysis. Notwithstanding the section 1605A plaintiffs need only to identify “the blocked assets” of the defendant sovereigns under this exception, 28 U.S.C. § 1610 note, they failed to raise the issue in district court.

Finally, we consider the plaintiffs’ claim to the IP addresses under all of the three exceptions. The district court did not reach the IP addresses. The plaintiffs contend that its silence amounts to an abuse of discretion but the district court’s failure to discuss the IP addresses is easily explained. In their self-styled “preliminary response” to ICANN’s motion to quash and their accompanying motion for extended discovery, the plaintiffs only twice referenced the IP addresses—once to claim “ICANN has presented virtually no facts concerning its role in the distribution of IP addresses or the ownership and value of IP addresses” and once to claim that “ICANN’s Motion to Quash does not address the economic value of IP addresses.” Pls.’ Response to ICANN’s Mot. to Quash at 7, 9. By contrast, the plaintiffs’ same submissions (their preliminary response and their discovery motion) referenced the ccTLDs 78 times, replete with allegations regarding ownership, monetary value and ICANN’s administrative role. In light of the plaintiffs’

omission of *any* argument touching on the IP addresses, the district court did not abuse its discretion in omitting to discuss them. On appeal, Amicus United States expressly doubted whether the plaintiffs had “preserved . . . arguments about IP addresses,” Br. for United States as *Amicus Curiae* at 19, which assertion the plaintiffs left unrebutted, *see* Br. for Appellants in Response to the United States as *Amicus Curiae*. We consider it waived on appeal. *See United States v. Olano*, 507 U.S. 725, 733 (1993) (“Whereas forfeiture is the failure to make the timely assertion of a right, waiver is the *intentional relinquishment or abandonment of a known right.*”) (emphasis added and internal quotations omitted).

To sum up, those plaintiffs seeking to attach the underlying judgments in *Haim I*, *Weinstein* and *Stern* have forfeited their claims *in toto*. Those plaintiffs seeking to attach the underlying judgments in *Haim II*, *Rubin*, *Wyatt* and *Calderon-Cardona* have forfeited all but their claim grounded in the terrorist activity exception to attachment immunity.

D. PROTECTION OF THIRD PARTY INTERESTS UNDER SECTION 1610(G)(3)

To this point we have assumed *arguendo* that D.C. law does not impede the plaintiffs’ pursuit of the defendant sovereigns’ ccTLDs. Moreover, the *Haim II*, *Rubin*, *Wyatt* and *Calderon-Cardona* plaintiffs have not forfeited reliance on the terrorist activity exception to attachment immunity vis-à-vis the ccTLDs. *See* 28 U.S.C. § 1610(g). Ordinarily, remand would be in order to allow the plaintiffs to continue discovery in an effort to establish whether the ccTLDs can properly be considered “property of” the defendants under the FSIA. *See* 28 U.S.C. § 1610(g)(1); *Heiser v. Islamic Republic*

of Iran, 735 F.3d 934 (D.C. Cir. 2013). Many critical issues remain disputed.²⁵

We assume without deciding that the ccTLDs the plaintiffs seek constitute “property” under the FSIA and, further, that the defendant sovereigns have some attachable ownership interest in them. Nonetheless, pursuant to the terrorist activity exception, the court has the “authority” to “prevent appropriately the impairment of an interest held by a

²⁵ For example, ICANN contends that the defendants do not own the .ir, .kp and .sy ccTLDs and that ICANN is therefore powerless to effect an attachment thereof. As discussed *supra* at 12–13, the plaintiffs submitted a declaration regarding their counsel’s discussion with an “internet infrastructure management and domain name systems operations and development expert” suggesting that ICANN had in the past “changed and redirected who runs certain ccTLDs . . . in conjunction with the ‘monetization’ of the ccTLDs by their respective governments, including instances where the governments transferred control away from academic communities to government approved third parties that acquired contractual property rights to exploit the ccTLD and generate revenue.” Gebelin Decl. at 2–3. There is also record evidence regarding the nation of Tuvalu’s monetization of its .TV ccTLD by sale or lease of its ccTLD management rights to a private company for millions of dollars. On the other hand, ICANN contends that ccTLDs are not property at all because they are “not an interest capable of precise definition, because [they are] always in flux,” Appellee’s Br. at 12, and that “there is, in fact, no established market within which ccTLDs are purchased and sold,” *id.* at 13–14. They also argue that no one has the requisite control over ccTLDs in order to establish ownership and that, in any event, “[a]uthoritative Internet protocol standards declare that concerns about rights and ownership of domains are inappropriate.” *Id.* at 12. Finally, the United States as amicus argues that the internet governance community “explicitly rejects efforts to assert property rights in [ccTLDs].” Br. for United States as *Amicus Curiae* at 11.

person who is not liable in the action giving rise to a judgment”—*i.e.*, we are expressly authorized to protect the interests of ICANN and other entities. 28 U.S.C. § 1610(g)(3).²⁶ Because of the enormous third-party interests at stake—and because there is *no* way to execute on the plaintiffs’ judgments without impairing those interests—we cannot permit attachment.²⁷

The plaintiffs demand, in effect, that ICANN delegate management of the “.ir” ccTLD²⁸ so that they can “sell or license the operation of the ccTLD[] to a third party.” Appellants’ Reply Br. at 26. As explained, the power to operate a ccTLD includes the power to register (or remove) domain names from that registry. Thus, an entity seeking a

²⁶ Although the two FSIA exceptions to attachment immunity the plaintiffs have either forfeited or waived do not include a similar provision, this case does not turn on forfeiture/waiver. Only the terrorist activity exception permits attachment “regardless of,” *inter alia*, “whether th[e] [defendant] government is the sole beneficiary in interest of the property,” 28 U.S.C. § 1610(g)(1)(D). And according to the *expressio unius est exclusio alterius* canon of statutory construction, that the terrorist activity exception expressly provides for attachment of such property suggests that the other exceptions require that the defendant sovereign have a more complete ownership interest. Although we express no view on whether and to what extent the defendant sovereigns, ICANN or any other party can “own” the ccTLDs, it seems plain that satisfying the other exceptions requires a more substantial ownership interest than does this exception.

²⁷ Moreover, although we do not find it necessary to reach the issue, the United States may be a necessary party hereto and, if so, this fact would provide another reason for quashing the writs of attachment. *Arizona v. California*, 298 U.S. 558, 571–72 (1936).

²⁸ We use “.ir” (Iran) as an example to illustrate the interests at stake.

“.ir” domain name will have to register through the plaintiffs or their designee—a process in which the ccTLD manager can extract a fee. The plaintiffs’ plan plainly impairs the interests of “person[s] who [are] not liable in the action giving rise to [the] judgment” in myriad ways. 18 U.S.C. § 1610(g).

First, requiring ICANN to delegate “.ir” to the plaintiffs would bypass ICANN’s process for ccTLD delegation, which includes ensuring that the incoming manager has technical competence and a commitment to serving the Iranian Internet community’s interests. The plaintiffs and, more importantly, their prospective designee may not possess that technical competence or commitment. Granted, the plaintiffs are “aware that the . . . court can—and should—protect the interests of third parties” and they “welcome the opportunity to work together with the district court and ICANN to ensure a smooth transition.” Appellants’ Reply Br. at 26. But even if the plaintiffs are able to show adequate competence and commitment, the act of forced delegation *itself* impairs ICANN’s interest in “protect[ing] the stability . . . [and] interoperability . . . of the DNS.” Decl. of John O. Jeffrey, App’x 24.2 ¶ 5.

Recall that a change in the root zone file will only affect the routing of a search for “.ir.” But a change in the root zone file does not also transfer the information stored on the ccTLD server.²⁹ To ensure that any delegation occurs

²⁹ For example, assume there is now a web page with the domain name “example.ir,” meaning that the SLD “example” is registered within the “.ir” ccTLD. An end-user searching for “example.ir” reaches the web page by first querying the root servers for “.ir” and then the “.ir” server for the “example.ir” domain. The “.ir” server directs the end-user to “example.ir” because it knows the location of “example.ir,” that is, “example.ir” is registered within it. But, we may also assume, this web page is not currently

seamlessly, ICANN requires that the incoming manager provide a plan to preserve the stability of the ccTLD, which plan explains how existing registrants will be affected. According to ICANN, the current ccTLD managers in the defendant countries will not voluntarily transfer information regarding their registrants and, because the relevant servers are located abroad, we are powerless to so require them. If ICANN is required to direct an end-user looking for “.ir” web pages to the plaintiffs’ server but the plaintiffs are unable to direct them to the requested SLD, the Internet’s stability and interoperability are undermined.³⁰

The impairment does not end there. As the plaintiffs recognize, ICANN occupies its position only because “the global community *allows it* to play that role.” Appellants’ Br. at 34 (emphasis added). “[T]he operators of . . . top level domains” can “form a competitor to ICANN and agree to refer all DNS traffic to a new root zone directory.” *Id.*; see also Br. for United States as *Amicus Curiae* at 13 (“As a technological matter, nothing prevents an entity outside the United States from publishing its own root zone file and persuading the operators of the Internet’s name servers to treat that version as authoritative instead.”). This result,

registered within the *plaintiffs’* server which, post-delegation, would “host” the “.ir” ccTLD. Before the SLD is so registered, an end-user searching for “example.ir” is not able to reach the web page. Although it would remain accessible through the *old* “.ir” server (*i.e.*, Iran’s server), the root servers, as a result of the delegation, would no longer direct queries there.

³⁰ The plaintiffs do not allege that a particular ccTLD management has *ever* been transferred without the cooperation of the outgoing manager. *Cf.* Gebelin Decl. at 6, App’x at 54 (alleging Tuvalu transferred management of its ccTLD to monetize *its* interest).

known as “splitting the root,” is widely viewed as a potentially disastrous development; indeed, some regard it as the beginning of “ultimate collapse of Internet stability”—a “doomsday scenario for the globally accessible” network and, thus, for ICANN. Harold Feld, *Structured to Fail: ICANN and the ‘Privatization’ Experiment*, in WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION 351 (Cato Inst. 2003). Whether that description of a split root is accurate need not concern us; ICANN’s interests, as a third party “not liable in the action giving rise to [the] judgment,” 18 U.S.C. § 1610(g)(3), are sufficient for us to protect them pursuant to section 1610(g)(3) of the FSIA. *See* Appellee’s Br. at 34 (“[F]orced re-delegation of the Subject ccTLDs would . . . wreak havoc on the domain name system.”); *see also* Br. for United States as *Amicus Curiae* at 13 (“[T]he result would be devastating for ICANN, for the [current] model of Internet governance, and for the freedom and stability of the Internet as a whole.”).

But given that the ICANN-administered DNS is the beneficiary of substantial network effects,³¹ how could such a doomsday scenario arise? And why would forced delegation

³¹ “In markets characterized by network effects, one product or standard tends towards dominance, because the utility that an end-user derives from consumption of the good increases with the number of other agents consuming the good.” *United States v. Microsoft Corp.*, 253 F.3d 34, 49 (D.C. Cir. 2001) (internal quotations omitted). Here, the ICANN-administered DNS and the authoritative root zone file “tend towards dominance” because domain name registries “and end-users have powerful economic incentives to remain compatible and connected with each other.” Milton J. Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction*, 3 J. NETWORK IND. 313, 315 (2002).

hasten its arrival?³² In light of the plaintiffs' recognition that ICANN's control "stems only from the fact that the global community allows it to play that role," Appellants' Br. at 34, and considering that the delegation of the three defendant sovereigns' ccTLDs could likely antagonize the global community, *see* Br. for United States as *Amicus Curiae* at 13 ("It is not difficult to imagine that a court-ordered change to the authoritative root zone file at the behest of private plaintiffs would prompt members of the global Internet community to turn their backs on ICANN for good."), we believe the doomsday scenario is not beyond imagining.³³

³² As others have explained, "the deck is stacked so heavily in favor of an established root" that splitting is likely to occur only if "the existing root is doing something seriously wrong." *Competing DNS Roots*, *supra* n.31, at 315.

³³ As noted earlier, an end-user ISP ordinarily uses DNS protocols to ask the root servers for the location of one of the DNS's TLDs. But there is no technological barrier binding ISPs to the DNS. A sovereign has authority over ISPs operating in its country and can "act[] unilaterally to redirect Internet traffic" for end-users within its borders "by requiring Internet service providers . . . to use what amounts to [that] government's own DNS." Harold Feld, *Structured to Fail: ICANN and the 'Privatization' Experiment*, in WHO RULES THE NET?: INTERNET GOVERNANCE AND JURISDICTION 354 (Cato Inst. 2003). For example, a foreign government can require that, when receiving a query for a particular TLD, an ISP operating within its borders *not* direct that query to a root server but rather to a different location altogether. If ICANN delegates management of ".ir" to the plaintiffs and the *plaintiffs* control where a query for ".ir" SLDs is directed, Iran has a powerful incentive to require its ISPs to bypass the root servers altogether and instead require ISPs to direct queries to the server that formerly hosted the ".ir" ccTLD. Under that circumstance, end-users in Iran and other parts of the world might access *different* web pages by querying *identical* domain names.

34

For the foregoing reasons, the judgment of the district court is affirmed.

So ordered.

And there is no reason to suppose that “members of the global Internet community [would not] turn their backs on ICANN for good.” Br. for United States as *Amicus Curiae* at 13. For example, another sovereign whose citizens do business through web pages registered under the former “.ir” ccTLD might no longer permit *their* ISPs to search the root servers for “.ir” SLDs. Whether or not this possibility is a positive development for the Internet, it unquestionably impairs ICANN’s interests in “protect[ing] the stability . . . [and] interoperability . . . of the DNS,” Decl. of John O. Jeffrey, App’x 24.2 ¶ 5.