

Section-by-Section Summary of the Foreign Anti-Digital Piracy Act (FADPA)

Introduced by Rep. Zoe Lofgren (D-CA-18)

Section 1: Short Title

- The Act may be cited as the "Foreign Anti-Digital Piracy Act" (FADPA).
-

Section 2: Blocking Orders Relating to Infringing Foreign Websites or Online Services

- **Amends Title 17 of the U.S. Code** to allow copyright owners to petition U.S. courts for no-fault injunctions blocking access to infringing foreign websites or online services.
-

§ 502A. Blocking Orders for Specifically Identified Infringing Foreign Websites or Online Services

(a) Preliminary Order

1. Petition for Preliminary Order

- A copyright owner or exclusive licensee may file a petition in U.S. District Court to obtain a preliminary order against a foreign website or online service engaging in copyright infringement.
- The petition must show that:
 - For non-live content: The transmission of a work through a foreign website likely infringes exclusive rights under Section 106 and is causing irreparable harm.
 - For live events: If an imminent or ongoing unauthorized transmission of a live event is likely to infringe, and will cause irreparable harm, the petitioner may seek an order.

2. Issuance of Preliminary Order

- The court must find the following to issue a preliminary order:
 - The foreign website or online service is identified by domain name, IP address, or similar identifier.
 - The petitioner has attempted to serve notice to the website's operator.
 - The petitioner has notified service providers that facilitate access to the infringing website.
 - The operator is outside the U.S. or cannot be determined to be within the U.S.
 - The website is primarily designed for infringement, has no commercially significant purpose other than infringement, or is intentionally marketed for infringing use.

- The petitioner has attested under penalty of perjury to the accuracy of its claims and has a substantial interest in enforcing its rights.

3. **Non-Issuance of Preliminary Order**

- A court may not issue a preliminary order if the infringing activity has ceased entirely and is unlikely to resume.

4. **Contesting the Preliminary Order**

- The operator of the foreign website or online service has 30 days to appear in court and contest the order.

5. **Special Master Appointment**

- If the operator does not appear, the court may appoint a special master with the authority to gather and review publicly available information to assist the court in determining whether the criteria in paragraph (2) have been satisfied to grant the order.

6. **Expedited Review for Live Events**

- The court must act on a petition within a specified timeframe:
 - **Standard Review:** After a 14-day reply period following the filing of an opposition.
 - **No Opposition:** The court may issue an order after the opposition period expires.
 - **Live Events:** If the transmission of a live event is imminent or ongoing, the court must act on an expedited basis to address the imminent or continuing harm.

7. **Ex Parte Orders for Live Events**

- If a foreign website or online service is engaged in the imminent or ongoing unauthorized transmission of a live event, the court may issue an order on an ex parte basis.

(b) Blocking Orders to Prevent Access to Foreign Website or Online Service

1. **Motion for Blocking Order**

- After obtaining a preliminary order, the copyright owner may request the court to issue a blocking order requiring service providers to take reasonable and technically feasible steps to prevent access to the infringing foreign website or online service.

2. **Issuance of Blocking Order**

- The court must find that blocking the site will not:
 - Interfere with access to non-infringing content.
 - Significantly burden the service provider.
 - Disserve the public interest.
- **(B) Terms and Conditions of the Order:**
 - **Compliance Timelines:**

- i. For orders not related to the imminent public performance of a live event:
 - Service providers must comply within 15 days of the order’s issuance.
 - If the court finds good cause, compliance may be extended to 20 days.
 - ii. For orders related to an imminent live event,
 - Compliance must occur within a timeframe that accounts for:
 - The imminent nature of the infringement.
 - The capabilities of the service provider.
 - Technical feasibility of implementation.
 - Compliance must occur no later than 7 days after issuance.
- **Expiration of the Order:**
 - i. 12 months after the service provider is served, unless extended by the court.
 - ii. If the order relates to one live event, it expires 48 hours after the event concludes.
 - iii. the order relates to multiple live events, it expires 48 hours after the final event concludes.
- **(C) Limitations on the Order:**
 - The order may not:
 - i. Prescribe specific technical measures for compliance.
 - ii. Require service providers to take actions that would prevent users from using virtual private networks (VPNs).

3. Amending Orders to Add Service Providers

- Petitioners may seek to amend orders to apply to additional service providers if:
 - The provider was not included in the original order.
 - The provider now facilitates access to the infringing site.

4. Amending Orders to Add Additional Domain Names or IP Addresses

- Unless otherwise determined by the court, petitioners may update the blocking order by direct notification to ISPs if:
 - The infringing site moves to a new domain name or IP address.
 - The site employs circumvention techniques to evade the order.

5. Implementation and Review of Blocking Orders

- Courts limit review of service provider compliance to whether their actions were unreasonable or in bad faith.
- Providers may temporarily suspend blocking orders:
 - To correct or investigate whether the implementation of the order by the service provider is preventing access to a website or online service other than the foreign online website or online service identified in the order.
 - To maintain network integrity or quality of the network or operations of the service provider.
- **Cost Reimbursement:** Upon a motion by a service provider served with an order issued under subsection (c), the court may require the petitioner to pay reasonable marginal costs and

expenses directly incurred in implementing and complying with the order. This does not include capital expenditures, costs and expenses incurred with respect to infrastructure, and attorney fees.

6. **Extension of Blocking Orders:** Orders not related to live events may be extended for up to 12 months if infringement continues.

7. **Transparency Provisions**

- Courts must publish blocking orders on a publicly accessible website including:
 - The petitioner’s name.
 - The foreign website or online service being blocked.
 - The date and duration of the order.
 - A summary of the court’s findings.
- Courts may redact sensitive information to prevent circumvention or risks to national security, personal safety, or an ongoing law enforcement investigation.

8. **Service Provider Immunity**

- **Liability Protections:** A service provider in compliance with a court order under this section may not be held liable for:
 - (i) Any injury alleged by a foreign website, online service, or its users resulting from measures taken to implement the order.
 - (ii) Any injury alleged by a foreign website, online service, or its users due to actions taken (or not taken) in good faith by the service provider in implementing the order based on information provided under this subsection.
 - (iii) Any injury alleged by an operator of a foreign website or online service identified in the order, even if later determined to have been inaccurately identified or not meeting the criteria for an order.
 - (iv) Any copyright infringement claim against the service provider brought by the copyright owner who obtained the order, if the claim is based on the provider’s role in providing access to the foreign website or service before the enactment of FADPA.
- **Evidentiary Protection:**
 - The issuance of an order identifying a service provider or a court finding that the provider complied with the order may not be used as evidence in court to allege the provider engaged in copyright infringement.

(c) Preservation of Safe Harbor Protections:

- A service provider identified in a blocking order under this Act does not lose liability protection under Section 512(a) (Digital Millennium Copyright Act “DMCA” safe harbor) solely due to their identification in the order.

(d) Rule of Construction:

- Except as explicitly provided, this Act does not alter, reinterpret, or affect the application of any provision under Section 512 of Title 17 (Digital Millennium Copyright Act).

(e) Definitions

- 1) **COVERED PERSON:** a copyright owner or an exclusive licensee of a copyright owner.
- 2) **BROADBAND PROVIDER:** a provider of broadband internet access service, as defined in section 8.1(b) of title 47, Code of Federal Regulations (or any successor regulation)
 - that provides such service to 100,000 or more subscribers; and
 - is subject to or consents to the jurisdiction of the court.
- 3) **FOREIGN WEBSITE OR ONLINE SERVICE:** a website or online service operated by a foreign person.
- 4) **FOREIGN PERSON:** an individual— (A) physically located outside of the United States; or (B) whose physical location cannot be determined to be within the United States.
- 5) **LIVE EVENT:** an event that is performed publicly (such as a concert, sporting event, or award show).
- 6) **PUBLIC DOMAIN NAME RESOLUTION SERVICES:** domain name resolution services that are accessible to the general public. By specifically covering public DNS resolvers, this definition excludes private or internal DNS services used within closed network.
- 7) **SERVICE PROVIDER:** means
 - “(i) a broadband provider as defined above; and
 - “(ii) a provider of public domain name resolution services that has an annual revenue of over \$100 million and does not include—
 - Service providers that provide domain name system resolution functions or services exclusively through encrypted DNS protocols; or
 - Service providers service that exclusively provide virtual private network (VPN) services, or similar services that encrypt and route user traffic through intermediary servers; or
 - an operator of a premises, such as a coffee shop, bookstore, airline, private end-user network, library, or university, that acquires broadband internet access service from a provider or entity described under subparagraph (A) to enable patrons of the premises to access broadband internet service from the premises.
- 8) **TRANSMISSION OF A LIVE EVENT:** means the digital transmission of a live event—
 - (A) simultaneously or nearly simultaneously with the live occurrence or public performance of the event; and
 - (B) for a commercial purpose.
 - “(i) ‘digital transmission’ includes, but is not limited to, transmission by satellite broadcasting.
- 9) **VIRTUAL PRIVATE NETWORK:** means a service that establishes an encrypted connection between a device and a remote server that—
 - (A) routes the internet traffic of the user of such device through the remote server; and
 - (B) masks the internet protocol address of such user.
- 10) **WEBSITE OR ONLINE SERVICE:** a website or uniquely identifiable online location that is—
 - (A) accessible to the public within the United States; and
 - (B) identifiable by a single internet protocol address, a domain name, or other similar online identifier.

Effective Date:

- This Act shall take effect on the date that is six months after the date of the enactment of this Act.