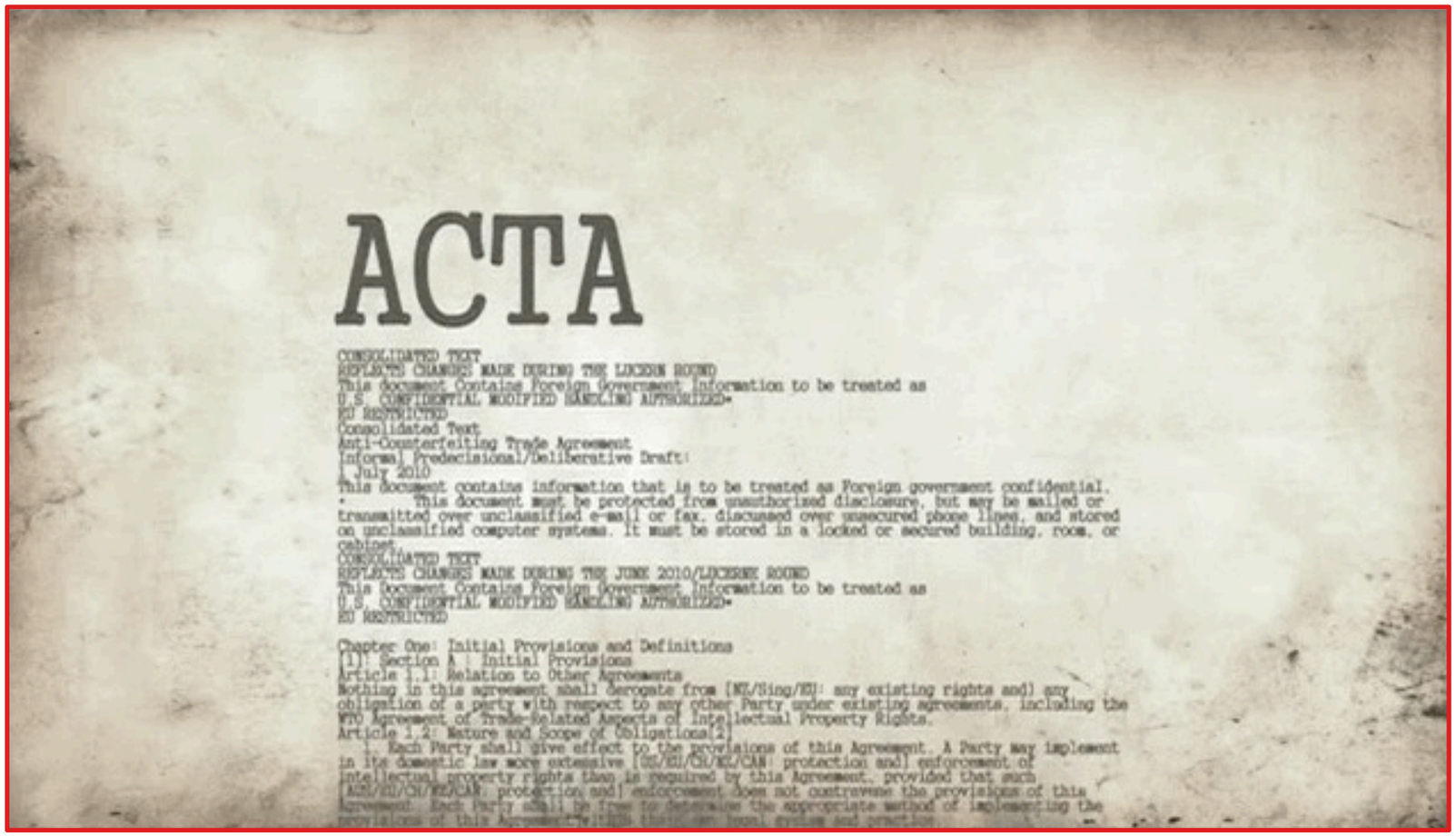
ACTA – PIPA – SOPA - impact on the internet?


DEPARTMENT OF JUSTICE
FBI ANTI-PIRACY
WARNING
FEDERAL BUREAU OF INVESTIGATION
NATIONAL INTELLECTUAL PROPERTY RIGHTS
IPR CENTER
COORDINATION CENTER
This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court.
A federal grand jury has indicted several individuals and entities allegedly involved in the operation of Megaupload.com and related websites charging them with the following federal crimes:
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

EMOTINALLY HIGH UP



ACTA

CONSOLIDATED TEXT
REFLECTS CHANGES MADE DURING THE LUCERN ROUND
This document Contains Foreign Government Information to be treated as
U.S. CONFIDENTIAL MODIFIED HANDLING AUTHORIZED.
EU RESTRICTED
Consolidated Text
Anti-Counterfeiting Trade Agreement
Informal Predecisional/Deliberative Draft:
4 July 2010
This document contains information that is to be treated as Foreign government confidential.
- This document must be protected from unauthorized disclosure, but may be mailed or transmitted over unclassified e-mail or fax, discussed over unsecured phone lines, and stored on unclassified computer systems. It must be stored in a locked or secured building, room, or cabinet.
CONSOLIDATED TEXT
REFLECTS CHANGES MADE DURING THE JUNE 2010/LUCERNE ROUND
This Document Contains Foreign Government Information to be treated as
U.S. CONFIDENTIAL MODIFIED HANDLING AUTHORIZED.
EU RESTRICTED

Chapter One: Initial Provisions and Definitions
[1] Section A : Initial Provisions
Article 1.1: Relation to Other Agreements
Nothing in this agreement shall derogate from [MX/Sing/EU: any existing rights and] any obligation of a party with respect to any other Party under existing agreements, including the WTO Agreement of Trade-Related Aspects of Intellectual Property Rights.
Article 1.2: Nature and Scope of Obligations[2]
1. Each Party shall give effect to the provisions of this Agreement. A Party may implement in its domestic law more extensive [US/EU/CH/MX/CAN: protection and] enforcement of intellectual property rights than is required by this Agreement, provided that such [MX/EU/CH/MX/CAN: protection and] enforcement does not contravene the provisions of this Agreement. Each Party shall be free to determine the appropriate method of implementing the provisions of this Agreement within their own legal system and practice.

ACTA wikipedia

- The Anti-Counterfeiting Trade Agreement (ACTA) is a multinational treaty for the purpose of establishing international standards for intellectual property rights enforcement. **The agreement aims to establish an international legal framework for targeting counterfeit goods, generic medicines and copyright infringement on the Internet,** and would create a **new governing body outside existing forums**, such as the World Trade Organization, the World Intellectual Property Organization, or the United Nations.
- The agreement was signed in October 2011 by Australia, Canada, Japan, Morocco, New Zealand, Singapore, South Korea and the United States. In January 2012, the European Union and 22 countries which are member states of the European Union signed as well, bringing the total number of signatories to 31. After approval (ratification) by 6 countries, the convention will come into force.
- Supporters have described the agreement as a **response to "the increase in global trade of counterfeit goods and pirated copyright protected works"**. Large intellectual property-based organizations such as the MPAA and Pharmaceutical Research and Manufacturers of America were active in the treaty's development.

http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement

ACTA how it developed

- Not in a stand way in an international body

- **Apart from the participating governments, an advisory committee of large US-based multinational corporations was consulted on the content of the draft treaty.** (including the Pharmaceutical Research, International Intellectual Property Alliance...)
- ACTA was first developed by Japan and the United States in 2006.
- Canada, the European Union (represented in the negotiations by the European Commission, the EU Presidency and EU Member States.) and Switzerland joined the preliminary talks throughout 2006 and 2007.
- Official negotiations began in June 2008, with Australia, Mexico, Morocco, New Zealand, the Republic of Korea and Singapore joining the talks.
- Mexico withdrew Mexico from ACTA negotiations on 30 September 2010.

ACTA content and layout

- **Chapter I**: **Initial Provisions and General Definitions**
  - scope of the agreement
  - relations to other agreements.
  - It asserts that obligations from other agreements still exist with entry into force of this agreement
  - applies only those intellectual property rights existing in the country applying the treaty
  - Countries may impose stricter measures than the treaty requires
  - should share (confidential) information for law enforcement purposes
  - The treaty explicitly also applies to Free Zones .
- **Chapter II**: **Legal Framework** for Enforcement of Intellectual Property Rights
  - Chapter II is divided in five sections.
- **Section 1**: **General Obligations**
  - **requirements to implement** the provisions in law
  - to have **fair procedure** as well as "proportionality between the seriousness of the infringement, the interests of third parties, and the applicable measures, remedies and penalties"

15 April 2011 - 6 chapters with 45 articles

ACTA content and layout

- **Section 2: Civil Enforcement**
  - rights holders have **access to civil or administrative procedures** and possibility for judges "*to issue an order against a party to desist from an infringement*".
  - judges **may also require** in civil procedure pirated copyright goods and counterfeit trademark **goods to be destroyed**.
  - judges **may ask (alleged) infringers to provide information on the goods** it "controls".
    - *see Hutter Singapore - KGB*
  - a Party's judicial authorities may consider inter alia **any legitimate measure of value submitted by a rights holder**, including lost profits, the value of infringed property as per market price, or the suggested retail price.
    - *highly critizized clause*

ACTA content and layout

- **Section 3: Border Measures**
  - At borders, officials may act on suspect goods **on their own initiative** or **upon request** of a "rights holder".
  - For goods **in transit,** the requirements **do not have to enacted by a state**.
  - "Small consignment" for commercial use are included in the border provisions
  - "goods of a non-commercial nature contained in travellers' personal luggage" are excluded from the scope.

ACTA content and layout

- **Section 4: Criminal Enforcement**
- **Article 23: Criminal Offenses**
  - At least "**wilful trademark counterfeiting or copyright or related rights piracy on a commercial scale**" should be punishable under criminal law.
    - *According to European Digital Rights, the article "provides an extremely low threshold" when considering that the scope includes "acts" and because consequences for infringement can include criminal penalties.*
- **Article 24: Penalties**
  - Penalties that Parties should have in their criminal system should **"include imprisonment as well as monetary fines",** which are **sufficiently high for discouragement** of actions forbidden under the treaty.

ACTA content and layout

- **Section 5: Enforcement of Intellectual Property Rights in the Digital Environment**
- **Article 27: Enforcement in the Digital Environmen**t
  - In the digital environment, also **Civil and Criminal enforcement should be available** "to permit effective action against an act of infringement of intellectual property rights which takes place in the digital environment".
  - Infringement over digital networks should be enforced **in a manner, which "preserves fundamental principles such as freedom of expression, fair process, and privacy**" .
  - **Against circumvention** of systems to prevent copying **measures** should be implemented
    - Critics of this article, such as the European Digital Rights, have raised concerns that its emphasis on the role of corporations in enforcement "promotes the policing and even punishment of alleged infringements outside normal judicial frameworks", while failing effective to "ensure effective remedies against such interferences with fundamental rights"

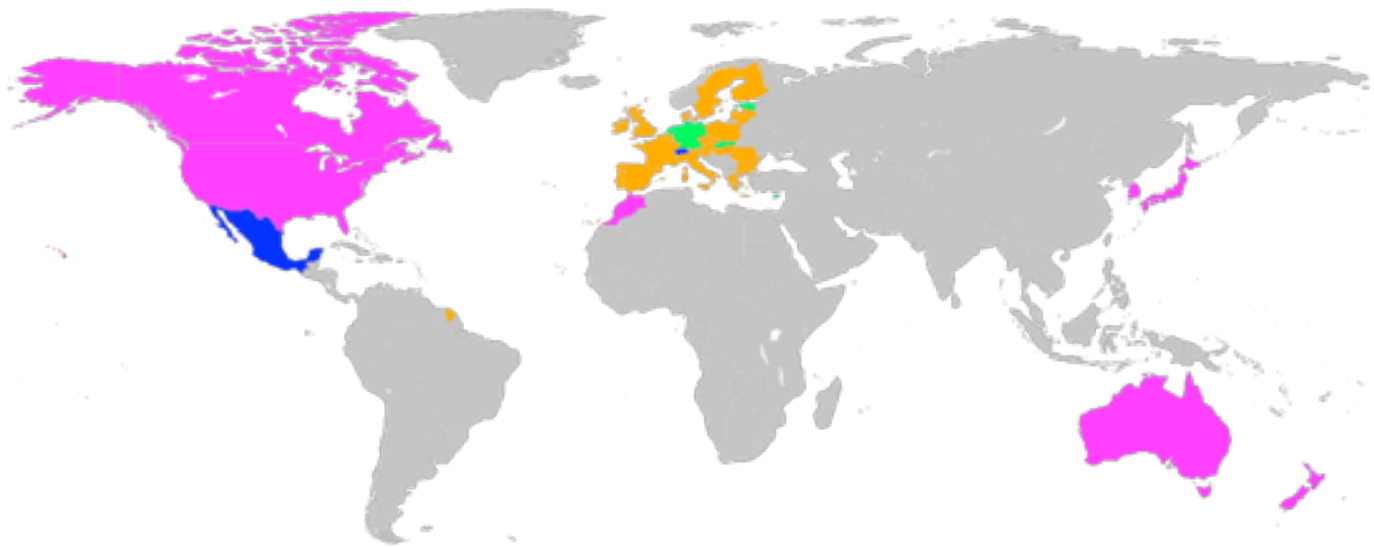
ACTA content and layout

- **Chapter III: Enforcement Practices**
- **Article 28: Enforcement Expertise**, Information, and Domestic Coordination
  - Parties are expected to **cultivate expertise within agencies tasked** with enforcing intellectual property rights, promote internal coordination, and facilitate joint actions.
  - They are also compelled to **collect and utilize statistical data,** as well as "other relevant information concerning intellectual property rights infringements", to prevent and combat infringement as necessary.
  - The article also indicates that parties shall "endeavour to promote, where appropriate, the **establishment and maintenance of formal or informal mechanisms**, such as advisory groups, whereby [their] competent authorities may receive the views of right holders and other relevant stakeholders."

ACTA content and layout

- **Article 42: Amendments**
  - Parties may submit proposed amendments to the Committee for review, which would then determine whether or not the proposed amendment should be presented for potential ratification, acceptance, or approval. Successful amendments would become **effective 90 days after all parties have provided their respective instruments of ratification, acceptance, or approval** to the depositary.

the ACTA landscape



Type	Plurilateral agreement
Drafted	15 November 2010 (final revision) [1] 15 April 2011 (formal publication) [2]
Signed	1 October 2011
Location	Tokyo
Effective	not in force
Condition	ratification by six states
Negotiators	Australia, Canada, the European Union, Japan, Mexico, Morocco, New Zealand, Korea, Singapore, Switzerland and the United States
Signatories	United States, the European Union and 22 of its Member States, Australia, Canada, Japan, Morocco, New Zealand, Singapore, and South Korea
Ratifiers	None
Depositary	Government of Japan
Languages	English, French and Spanish

protest against ACTA

THE JANUARY 18 BLACKOUT / STRIKE

IN NUMBERS AND SCREENSHOTS

January 18th was unreal. Tech companies and users teamed up. Geeks took to the streets. Tens of millions of people who make the internet what it is joined together to defend their freedoms. The network defended itself. Whatever you call it, we changed the politics of interfering with the internet forever--there's no going back.

Karel De Gucht's Fake ACTA Debate

Submitted on 29 Feb 2012 - 13:31
Tags: ACTA, IPRED, enforcement, Net filtering, De Gucht, dossier

Printer-friendly version | Send to friend

Last week, the Trade Commissioner De Gucht, the same who recently declared he was "not afraid of the anti-ACTA demonstrations", went on to explain why, considering the wave of criticism on ACTA, he is now turning to the European Court of Justice to assess whether ACTA would be detrimental to fundamental rights[1].

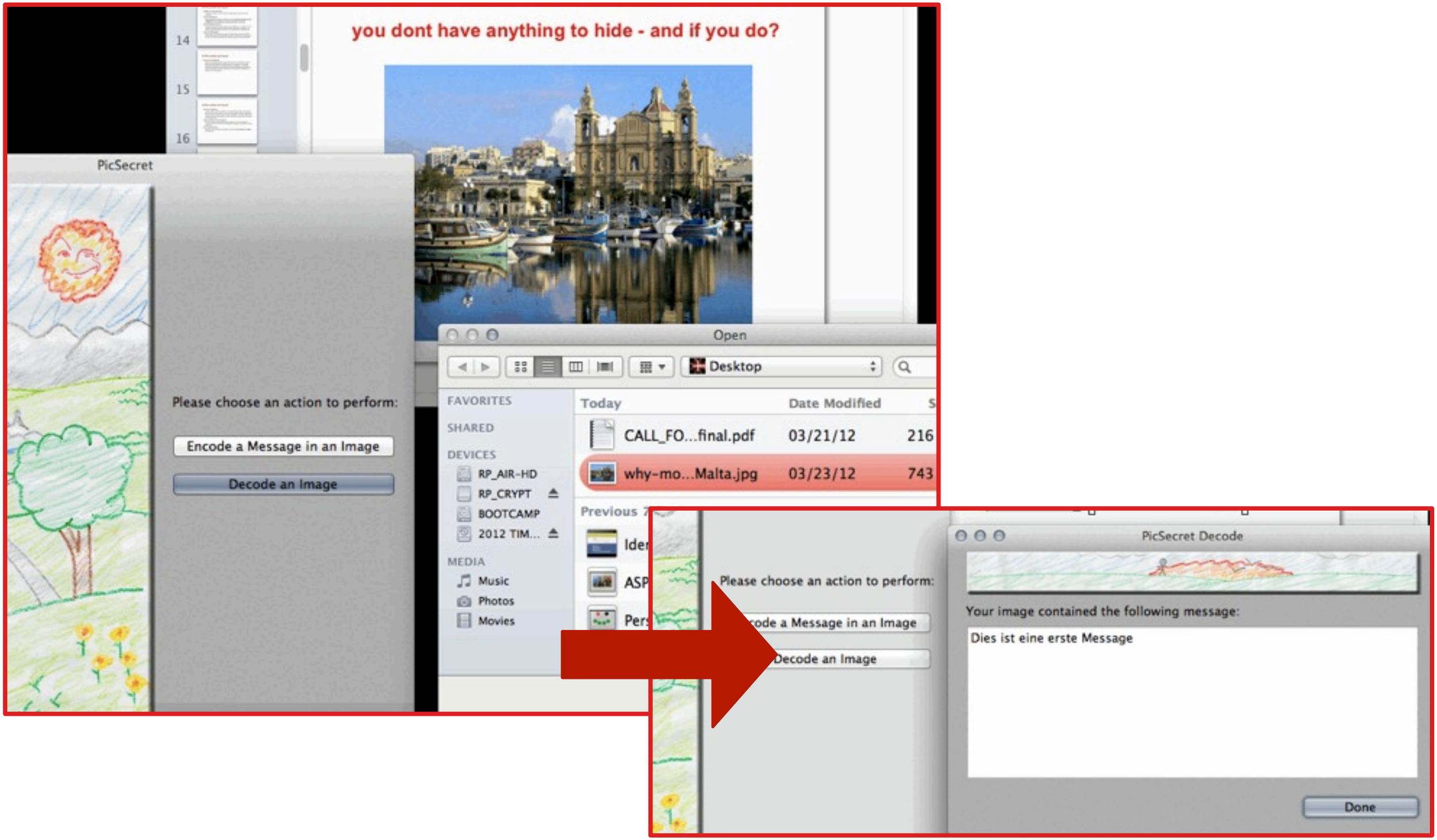
Commissioner DeGucht speaks about a balance to find between fundamental rights: between freedom of expression, privacy, "including the right to property, in case intellectual property"[2], assuming that copyright would deserve the same standing that the fundamental freedoms of persons, such as the freedom of expression.

De Gucht is actually trying to cover the tracks of his responsibility for the unacceptable ACTA. He is attempting to buy time, defuse opposition, and further manipulate any public debate on the reform of copyright. He characterizes the "Europe-wide debate on ACTA" as dominated by "disinformation on social media and blogs", as if the only-reasonable debate were one in which people agree with him. His defence of ACTA is based on 2 core arguments:

- ACTA does not change anything in Europe and will not change the way in which European citizens use websites and social media; and
- ACTA will change something for Europe as it will ensure that the jobs of Europeans will not be lost to the €200 billion of counterfeited goods (sic) flooding the markets.

you dont have anything to hide - and if you do?

ACTA AND STEGANOGRAPHY



WOULD YOU USE?

crypto if you have
something to hide?

if you really have
something to hide
crypto is not best as
it provokes suspicion

IT IS ABOUT CYBER - ALTERNATIVES?

Howard Smith at London Cymer Nov 2011:
80% can be prevented Computerhygene

It is more about prevention

Very big issue: different jusrisdictions making it impossible to follow up

Possibly securing and making transparent the origin would be helpful
like DNSSEC (obligation when it comes to eBusiness?)
like jurisdicton aware transport layers?

* * **PROBLEM SPAM**
* * **PROBLEM DISTANT CONTRACTS**

PIPA

Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011

SHOULD WE SET A SIGN OR A BAR ?

Full title	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011
Acronym	PIPA
Colloquial name(s)	Senate Bill 968

Citations

Codification

Legislative history

- **Introduced in the Senate as by** Patrick Leahy (D-VT) **on** May 12, 2011

Major amendments

None

Supreme Court cases

None

V • T • E

PIPA WIKIPEDIA

http://en.wikipedia.org/wiki/PROTECT_IP_Act

- The PROTECT IP Act (**Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, or PIPA**) is a proposed law with the stated goal of **giving the US government and copyright holders additional tools to curb access to "rogue websites dedicated to infringing or counterfeit goods",** especially those registered outside the U.S.[1] The bill was introduced on May 12, 2011, by Senator Patrick Leahy (D-VT)[2] and 11 bipartisan co-sponsors. The Congressional Budget Office estimated that implementation of the bill **would cost the federal government $47 million through 2016**, to cover enforcement costs and the hiring and training of 22 new special agents and 26 support staff. The Senate Judiciary Committee passed the bill, but Senator Ron Wyden (D-OR) placed a hold on it.
  - The PROTECT IP Act **is a re-write of** the Combating Online Infringement and Counterfeits Act (**COICA**), which failed to pass in 2010. **A similar House version** of the bill, the Stop Online Piracy Act (SOPA), was introduced on October 26, 2011.
  - In the wake of online protests held on January 18, 2012, Senate Majority Leader Harry Reid announced that a vote on the bill would be postponed until issues raised about the bill were resolved.

PIPA „the highlights“

- „information location tool shall take technically feasible and reasonable measures, as expeditiously as possible, to remove or disable access to the Internet site associated with the domain name set forth in the order“
- Nonauthoritative domain name servers would be ordered to take technically feasible and reasonable steps to prevent the domain name from resolving to the IP address of a website that had been found by the court to be "dedicated to infringing activities.“
- The website could still be reached by its IP address, but links or users that used the website’s domain name would not reach it.
  - BLACK MARKET /BLAK SERVICES

- OPPSERS Mozilla Corporation, Facebook, Electronic Frontier Foundation, Yahoo!, eBay, American Express, reddit, Google, Reporters Without Borders, Human Rights Watch, English Wikipedia ...

PIPA content

- **ENHANCING ENFORCEMENT AGAINST ROGUE WEBSITES OPERATED AND REGISTERED OVERSEAS.**

✤(a) COMMENCEMENT OF AN ACTION.

- (1) **IN PERSONAM.**
  The Attorney General may commence an in personam **action against**
- (A) a **registrant of a nondomestic domain name** used by an Internet site dedicated to infringing activities; or
- (B) an **owner or operator of an Internet site** dedicated to infringing activities accessed through a non-domestic domain name.
- (2) **IN REM.**
  If through due diligence the Attorney General is **unable to find a person** described in subparagraphs (A) or (B) of paragraph (1), **or no such person found** has an address **within a judicial district** of the United States, the Attorney General may commence an **in rem action against** a non-domestic **domain name** used by an Internet site dedicated to infringing activities.

PIPA content

- (b) ORDERS OF THE COURT.
  - **(1) IN GENERAL.**
    On application of the Attorney General following the commencement of an action under this section, the **court may issue** a temporary restraining order, a preliminary injunction, or an injunction, in accordance with rule 65 of the Federal Rules of Civil Procedure, **against the non-domestic domain name used by an Internet site dedicated to infringing activities**, **or against a registrant of such domain name, or the owner or operator of such Internet site** dedicated to infringing activities, **to cease and desist from undertaking any further activity** as an Internet site dedicated to infringing activities, if
    - ★(A) the **domain name is used within the United States to access such Internet site**; and
    - ★(B) the Internet site
      - ✳(i) **conducts business directed to residents** of the United States; and
      - ✳(ii) **harms holders of United States intellectual property rights.**

PIPA content

- (2) **DETERMINATION BY THE COURT.**
  For purposes of determining whether an Internet site conducts business directed to residents of the United States under paragraph (1)(B)(i), a **court may consider,** among other indicia, whether
  - ★(A) the Internet site is **providing goods or services** described in section 2(7) to users located in the United States;
  - ★(B) there is **evidence** that the Internet site is **not intended** to provide
    - ✳(i) such goods and services to users located in the United States;
    - ✳(ii) access to such goods and services to users located in the United States; and
    - ✳(iii) delivery of such goods and services to users located in the United States;
  - ★(C) the Internet **site has reasonable measures in place** to prevent such goods and services from being accessed from or delivered to the United States;
  - ★(D) the Internet site offers services obtained in the United States; and
  - ★(E) any prices for **goods and services are indicated in the currency of the United States**.

PIPA content

- (d) REQUIRED ACTIONS BASED ON COURT ORDERS.
  - (1) SERVICE.
    A Federal law enforcement officer, with the prior approval of the court, may **serve a copy of a court order issued pursuant to this section on** similarly situated entities within each class described in paragraph (2). Proof of service shall be filed with the court.
  - (2) REASONABLE MEASURES.
    After being served with a copy of an order pursuant to this subsection:
    - (A) OPERATORS.
      - (i) **IN GENERAL.**
        An **operator** of a nonauthoritative domain name system server shall take the least burdensome technically feasible and reasonable measures designed to **prevent the domain name described in the order from resolving** to that domain name's Internet protocol address, **except** that
        - (I) such operator shall **not be required**
          - (aa) **other than** as directed under this subparagraph, **to modify its network, software, systems, or facilities**;

PIPA content

- (bb) to **take any measures** with respect to domain name **lookups not performed by its own domain name server or domain name system servers located outside the United States**; or
- (cc) to **continue to prevent access to a domain name to which access has been effectively disable by other means**; and

◉(II) nothing in this subparagraph shall affect the limitation on the liability of such an operator under section 512 of title 17, United States Code.

✳(ii) TEXT OF NOTICE.
The **Attorney General shall prescribe the text of the notice** displayed to users or customers of an operator taking an action pursuant to this subparagraph. **Such text shall specify that the action is being taken pursuant to a court order obtained by the Attorney General.**

★(B) FINANCIAL TRANSACTION PROVIDERS.
A **financial transaction provider shall** take reasonable measures, as expeditiously as reasonable, designed to **prevent, prohibit, or suspend its service from completing payment** transactions involving customers located within the United States and the **Internet site associated with the domain name** set forth in the order.

PIPA content

★ (C) INTERNET ADVERTISING SERVICES.
An **Internet advertising service** that contracts with the Internet site associated with the domain name set forth in the order to provide advertising to or for that site, or which knowingly serves advertising to or for such site, shall take technically feasible and reasonable measures, as expeditiously as reasonable, designed to

- ✳(i) **prevent its service from providing** advertisements to the Internet site associated with such domain name; or
- ✳(ii) **cease making available advertisements** for that site, or paid or sponsored search results, links or other placements that provide access to the domain name.

★(D) INFORMATION LOCATION TOOLS.
An information location tool shall **take technically feasible and reasonable measures**, as expeditiously as possible, to

- ✳(i) r**emove or disable access** to the Internet site associated with the domain name set forth in the order; or
- ✳(ii) **not serve a hypertext link to such Internet site**.

PIPA content

- (3) COMMUNICATION WITH USERS.
  Except as provided under paragraph (2)(A)(ii), an **entity taking an action described in this subsection shall determine whether and how to communicate** such action to the entity's users or customers.
- (4) RULE OF CONSTRUCTION.
  For purposes of an action commenced under this section, the obligations of an entity described in this subsection shall be limited to the actions set out in each paragraph or subparagraph applicable to such entity, **and no order issued pursuant to this section shall impose any additional obligations** on, or require additional actions by, such entity.
- (5) ACTIONS PURSUANT TO COURT ORDER.
  - ★(A) IMMUNITY FROM SUIT.
    No cause of action shall lie in any Federal or State court or administrative agency **against any entity receiving a court order issued under this subsection**, **or against any director, officer, employee, or agent thereof, for any act reasonably designed to comply with this subsection or reasonably arising from such order,** other than in an action pursuant to subsection (e).

PIPA content

★(B) IMMUNITY FROM LIABILITY.
Any **entity receiving an order** under this subsection, and any director, officer, employee, or agent thereof, **shall not be liable to any party for any acts reasonably designed to comply with this subsection or reasonably arising from such order, other than in an action** pursuant to subsection (e), and any actions taken by customers of such entity to circumvent any restriction on access to the Internet domain instituted pursuant to this subsection or any act, failure, or inability to restrict access to an Internet domain that is the subject of a court order issued pursuant to this subsection despite good faith efforts to do so by such entity shall not be used by any person in any claim or cause of action against such entity, other than in an action pursuant to subsection (e).

PIPA content

- **ELIMINATING THE FINANCIAL INCENTIVE TO STEAL INTELLECTUAL PROPERTY ONLINE.**
  - (a) IN GENERAL.
    No financial transaction provider or Internet advertising service **shall be liable for damages to any person for voluntarily taking any action described in section** 3(d) or 4(d) with regard to an Internet site if the entity acting in good faith and based on credible evidence has a reasonable belief that the Internet site is an Internet site dedicated to infringing activities.
  - (b) INTERNET SITES ENGAGED IN INFRINGING ACTIVITIES THAT ENDANGER THE PUBLIC HEALTH.
    - (1) REFUSAL OF SERVICE.
      A domain name registry, domain name registrar, financial transaction provider, information location tool, or Internet advertising service, acting in good faith and based on credible evidence, may stop providing or refuse to provide services to an infringing Internet site that endangers the public health.

counter PIPA activities

PIPA concerns

- Technical objections to DNS blocking and redirection
  - does it work?

- Civil liberties issues
  - is it proportionate

- Concern for user-generated sites
  - who can be made reliable

- Business and innovation issues
  - does it tap on IPR

PIPA and DNS blocking

- Brings up again prehaps heats up ICAN debate
  - who is in control public/private
  - Internet Governance and the EU

- Legal Autonomy of nations (versus DNS)
  - DNS - blocking and scope of jurisdictions

- Alternative DNS
  - the move might encourage alternatives - introducing further security risk

- „DNS – RETAINERS might show up“
  - is DNS blocking effective in „those communities“

DNS blocking

Blocking access with DNS is not effective

Using DNS as a tool to prevent access to resources does not work. In reality, any blocking, at any layer in the Internet Architecture, will always be a combination of not be effective and hurt more than what is the intention. And because of that the effectiveness varies.

Two examples:

1. A domain name is blocked in the resolver(s)
    - This will block not only the content on a specific URL, but all URLs that share the same domain name
    - This will not block access if other resolver(s) are in use, for example a resolver the user run themselves
2. An IP address is blocked in the routing system
    - This will block not only the content on a specific IP address, but everything using that IP address (including all virtual hosts)
    - This will not block the same content on other IP addresses and changing IP address is easy (keep same domain name)

But blocking in the DNS is specifically bad now when DNSSEC is introduced. The signatures in DNSSEC are designed in such a way that they indicate both existence and non-existence of a domain name. Blocking is a third category, and is simply not part of the DNSSEC architecture. Unknown things will happen if the applications that use DNSSEC. I might create such problems with non-existence responses that people will not turn on DNSSEC, which imply the collateral damage by use of blocking can be considerable.

http://stupid.domain.name/node/1248

- DNS blocking might jeopardize DNSSEC

PIPA and colateral damage

- Collateral damage: False Litigation – people who are opposing SOPA and PIPA believe that **neither piece of legislation would do enough to protect against** false accusations.
- Collateral Damage: Meanwhile, **sites that host user-generated content** will be under pressure to closely monitor users' behavior. It could be a huge liability for startups.
- Collateral Damage: "takes the **risk of frivolous litigation**… to the entire Internet."
- Collateral Damage: "a tremendous chilling effect on people trying to conduct political discourse and trying to use content in a fair use context."
- Collateral Damage: SOPA and PIPA, in their current forms would be **ineffective in dealing with rogue websites** and would entail significant "collateral damage" in terms of stifling innovation and attenuating free speech.

PIPA and NON US jurisdictions

- SOPA provisions are **designed to have an extra-territorial** effect in countries around the world.
- NON-U.S. businesses and websites could easily find themselves targeted by SOPA. The bill grants the U.S. "in rem" jurisdiction over **any website that does not have a domestic jurisdictional connection**.
- Millions rely on the legitimate sites that are affected by the legislation. **If non-Americans remain silent, they may ultimately find the sites and services they rely upon silenced by this legislation**.
- U.S. intellectual **property strategy has long been premised on exporting its rules to other countries**.

PIPA and jurisdictions

- different jurisdictions still will have different opinions in a specific situation

- **technology does not really allow for this differentiation**

- DNS shopping in countries not subscribing to ACTA / PIPA / SOPA spirit

- leading to unreliable secondary DNS being a major thread

PROVIDERS and censoring

- To what extent are providers oblidged to execute „censoring“
- Encryped content is evading censoring in any case
- Even more: Stega-Content poses immense problems
- Are **closed groups** (black communities...) favored by such legislation?
- How does **dynamic content** relate to this legislation / agreement?
  would it legally affect skype for example?

Who what is in the focus

- stakeholders are the content providers
- users needs and whishes are not in the focus

Will it be long term effective

- DNS is only half way
  - think of illegality of SPAM
- So far prohibitors did not really survive the internet
  - think of Crypto banning
  - think of key escrow
- It indirectly legalizes what some arab countries do and did
  - this has a potential of bouncing back

Can we learn from this

- enhancing legal certaintiy by enriching DNS with
- trusted source
- securing DNS

PERHAPS EUROPE SHOULD THINK ABOUT TECHNOLOGICAL VALID ALTERNATIVES BUT WILL THIS HAPPEN? see ONS

PIPA and APPs

- APPS as content providers
- APPS as location distorter
- APPS as DNS shadower

PIPA and legal agreements

- Nation a decides
- Nation a and Nation b do not generally recognize decisions by courts
- How to block DNS?

PIPA referral hiding

- http://www.youtube.com/watch?v=zWRvaatXTho (GERMAN)

- „Die Telefonprotokolle Vorlesung“
  - It is illegal to report on on ongoing trials
  - However: It is legal to academically discuss (and reflect in the media this dicussion) jusridical interesting background
  - As in this case „referral hiding“ could be used to circumvent in an analog way

ECJ Referral: No Legal Debate Will Make ACTA Legitimate

Submitted on 22 Feb 2012 - 14:54
Tags: ACTA, De Gucht, press release

Printer-friendly version | Send to friend | Français

Paris, February 22nd – **The European Commission just announced its intent to ask the European Court of Justice (ECJ) for an opinion on the conformity of ACTA with fundamental freedoms. Beyond the obvious intent to defuse the heated debate currently taking place, this move aims to make the ACTA discussion a mere legal issue, when the main concerns are political by nature.**

While the EU Commission has consistently refused to undergo an impact assessment of ACTA on fundamental freedoms, it is now scared of the growing citizen opposition to ACTA and has decided to buy time.

Even if the the ECJ referral text has not been published yet, its announced framing is narrow and legalistic in nature. Important questions will not be asked, and therefore be left unanswered:

- Can a wide-ranging interpretation of ACTA's criminal sanctions (for "infringement on a commercial scale", including "aiding and abetting") be used as a bullying weapon by the copyright industry to force Internet actors into deploying contract-based repressive measures?[1]
- What will be the impact on EU policy-making and public debate of casting in stone current repressive policies for which an impact study is still expected, and which are heavily criticized (such as the EUCD and IPRED)?
- Can such a body of policies, impacting EU policy-making, the free flow of information and the freedom to conduct business on the Internet be negotiated instead of democratically debated, and yet be legitimate?
- Is ACTA necessary as we are facing an open conflict between repressive copyright policies and fundamental freedoms, and that other paths could be taken, such as a positive reform taking into account new cultural practices?

SOPA

The **Stop Online Piracy Act** (**SOPA**) is a United States bill introduced by U.S. Representative Lamar S. Smith(R-TX) to expand the ability of U.S. law enforcement to fight online trafficking in copyrighted intellectual property and counterfeit goods. Provisions include the requesting of court orders to bar advertising networks and payment facilities from conducting business with infringing websites, and search engines from linking to the sites, and court orders requiring Internet service providers to block access to the sites. The law would expand existing criminal laws to include unauthorized streaming of copyrighted content, imposing a maximum penalty of five years in prison. A similar bill in the U.S. Senate is titled the PROTECT IP Act (PIPA).


SOPA

SOPA content

- **ACTION BY ATTORNEY GENERAL TO PROTECT U.S. CUSTOMERS AND PREVENT U.S. SUPPORT OF FOREIGN INFRINGING SITES.**
  - (a) Definition.
  - For purposes of this section, a foreign Internet site or portion thereof is a "**foreign infringing site**" if
  - (1) the Internet site or portion thereof is a U.S.-directed site and is used by users in the United States;
    - (2) the owner or operator of such Internet site is committing or facilitating the commission of criminal violations punishable under section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of title 18, United States Code; and
    - (3) the Internet site would, by reason of acts described in paragraph (1), be subject to seizure in the United States in an action brought by the Attorney General if such site were a domestic Internet site.
  - (b) **Action By The Attorney General**.
  - (1) IN PERSONAM.
    - The Attorney General may commence an in personam **action against**
      - (A) a **registrant of a domain name** used by a foreign infringing site; or
      - (B) an **owner or operator of a foreign infringing** site

SOPA content

- (2) IN REM.
  If through due diligence the Attorney General is **unable to find a person** described in subparagraph (A) or (B) of paragraph (1), or no such person found has an address within a judicial district of the United States, the Attorney General may commence an **in rem action against a foreign infringing site or the foreign domain name** used by such site.
- (3) NOTICE.
  Upon commencing an action under this subsection, the Attorney General shall **send a notice** of the alleged violation and intent to proceed under this section
  - (A) to the **registrant of the domain name** of the Internet site
    - (i) at the postal and electronic mail addresses appearing in the applicable publicly accessible database of registrations, if any, and to the extent such addresses are reasonably available; and
    - (ii) via the postal and electronic mail addresses of the registrar, registry, or other domain name registration authority that registered or assigned the domain name of the Internet site, to the extent such addresses are reasonably available; or

SOPA content

- (B) to **the owner or operator** of the Internet site
  - (i) at the primary postal and electronic mail addresses for such owner or operator that is provided on the Internet site, if any, and to the extent such addresses are reasonably available; or
  - (ii) if there is no domain name of the Internet site, via the postal and electronic mail addresses of the Internet Protocol allocation entity appearing in the applicable publicly accessible database of allocations and assignments, if any, and to the extent such addresses are reasonably available; or
  - (C) in any other such form as the court may provide, including as may be required by rule 4(f) of the Federal Rules of Civil Procedure.

- (4) SERVICE OF PROCESS.
  For purposes of this section, the actions described in this subsection shall constitute service of process.

SOPA content

- (c) Actions Based On Court Orders.
  - (1) SERVICE.
    A **process server on behalf of the Attorney General,** with prior approval of the court, may serve a copy of a court order issued pursuant to this section on similarly situated entities within each class described in paragraph (2). Proof of service shall be filed with the court.
  - (2) REASONABLE MEASURES.
    After being served with a copy of an order pursuant to this subsection, the following shall apply:

SOPA content

- A) SERVICE PROVIDERS.
  - (i) IN GENERAL.
    A service provider shall take **technically feasible and reasonable measures designed to prevent access** by its subscribers located within the United States to the foreign infringing site (or portion thereof) that is subject to the order, including measures designed to prevent the domain name of the foreign infringing site (or portion thereof) from resolving to that domain name's Internet Protocol address. Such actions shall be taken as expeditiously as possible, but **in any case within 5 days after being served** with a copy of the order, or within such time as the court may order.
  - (ii) LIMITATIONS.
    A service provider shall **not be required**
    - (I) other than as directed under this subparagraph, **to modify its network, software, systems,** or facilities;
    - (II) to take any **measures** with respect to domain name resolutions **not performed by its own** domain name server; or
    - (III) to continue to prevent access to a domain name to which access has been effectively disabled by other means.

SOPA content

- (iii) CONSTRUCTION.
  Nothing in this subparagraph shall affect the limitation on the liability of a service provider under section 512 of title 17, United States Code.
- (iv) TEXT OF NOTICE.
  The Attorney General shall prescribe the text of any notice displayed to users or customers of a service provider taking actions pursuant to this subparagraph. Such text shall state that an action is being taken pursuant to a court order obtained by the Attorney General.

- (B) INTERNET SEARCH ENGINES.
  A **provider of an Internet search** engine shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, **designed to prevent the foreign infringing site** that is subject to the order, or a portion of such site specified in the order, **from being served as a direct hypertext link**.

SOPA content

- (C) PAYMENT NETWORK PROVIDERS.
- (i) PREVENTING AFFILIATION.
  A **payment network provider** shall take technically feasible and reasonable measures, as expeditiously as possible, but in any case within 5 days after being served with a copy of the order, or within such time as the court may order, designed to **prevent, prohibit, or suspend its service from completing payment transactions involving customers located within the United States or subject to the jurisdiction of the United States** and the payment account
  - (I) which is used by the foreign infringing site, or portion thereof, that is subject to the order; and
  - (II) through which the payment network provider would complete such payment transactions.
  - (ii) NO DUTY TO MONITOR.
  - A payment network provider shall be considered to be in compliance with clause (i) if it takes action described in that clause with respect to accounts it has as of the date on which a copy of the order is served, or as of the date on which the order is amended under subsection (e).

SOPA content

- (3) COMMUNICATION WITH USERS.
  Except as provided under paragraph (2)(A)(iv), an entity taking an action described in this subsection shall determine the means to communicate such action to the entity's users or customers.
- (4) ENFORCEMENT OF ORDERS.
  - (A) IN GENERAL.
  - To **ensure compliance with orders** issued pursuant to this section, the Attorney General may bring an action for injunctive relief
    - (i) **against any entity served** under paragraph (1) that knowingly and willfully fails to comply with the requirements of this subsection to compel such entity to comply with such requirements; or
    - (ii) **against any entity** that knowingly and willfully provides or offers to provide a **product or service designed or marketed for the circumvention or bypassing** of measures described in paragraph (2) and taken in response to a court order issued pursuant to this subsection, to enjoin such entity from interfering with the order by continuing to provide or offer to provide such product or service.
  - (B) RULE OF CONSTRUCTION.
    The authority granted the Attorney General under subparagraph (A)(i) shall be the sole legal remedy to enforce the obligations under this section of any entity described in paragraph (2).

SOPA content

- (C) DEFENSE.
  A **defendant in an action** under subparagraph (A)(i) may establish an affirmative defense by showing that the defendant does **not have the technical means** to comply with this subsection without incurring an unreasonable economic burden, or that the order is not authorized by this subsection. Such showing shall not be presumed to be a complete defense but shall serve as a defense only for those measures for which a technical limitation on compliance is demonstrated or for such portions of the order as are demonstrated to be unauthorized by this subsection.
- (D) DEFINITION.
  For purposes of this paragraph, **a product or service designed or marketed for the circumvention or bypassing of measures** described in paragraph (2) and taken in response to a court order issued pursuant to this subsection **includes a product or service that is designed or marketed** to enable a domain name described in such an order
  - (i) **to resolve to that domain name's Internet protocol address notwithstanding the measures taken** by a service provider under paragraph (2) to prevent such resolution; or
  - (ii) **to resolve to a different domain name** or Internet Protocol address that the provider of the product or service knows, reasonably should know, or reasonably believes is used by an Internet site offering substantially similar infringing activities as those with which the infringing foreign site, or portion thereof, subject to a court order under this section was associated.

SOPA content

- (5) IMMUNITY.
  - (A) IMMUNITY FROM SUIT.
    Other than in an action pursuant to paragraph (4), **no cause of action** shall lie in any Federal or State court or administrative agency against any entity served with a copy of a court order issued under this subsection, or **against any director, officer, employee, or agent** thereof, for any act **reasonably designed to comply** with this subsection or reasonably arising from such order.
  - (B) IMMUNITY FROM LIABILITY.
    Other than in an action pursuant to paragraph (4)
    - (i) any **entity served** with a copy of an order under this subsection, and any **director, officer, employee, or agent** thereof, **shall not be liable** for any act reasonably designed to comply with this subsection or reasonably arising from such order; and
    - (ii) any
      - (I) **actions taken by customers** of such entity to circumvent any restriction on access to the foreign infringing site, or portion thereof, that is subject to such order, that is instituted pursuant to this subsection, or
      - (II) **act, failure, or inability to restrict access** to a foreign infringing site, or portion thereof, that is subject to such order, in spite of good faith efforts to comply with such order by such entity,

    shall not be used by any person in any claim or cause of action against such entity.

SOPA content

- **SEC. 103. MARKET-BASED SYSTEM TO PROTECT U.S. CUSTOMERS AND PREVENT U.S. FUNDING OF SITES DEDICATED TO THEFT OF U.S. PROPERTY.**
  - (a) Definitions.
    In this section:
    - (1) DEDICATED TO THEFT OF U.S. PROPERTY.
      An “Internet site is dedicated to theft of U.S. property” if
      - (A) it is an Internet site, or a portion thereof, that is a U.S.-directed site and is used by users within the United States; and
      - (B) either
      - (i) the U.S.-directed site is primarily designed or operated for the purpose of, has only limited purpose or use other than, or is marketed by its operator or another acting in concert with that operator for use in, offering goods or services in a manner that engages in, enables, or facilitates
      - (I) a violation of section 501 of title 17, United States Code;
      - (II) a violation of section 1201 of title 17, United States Code; or
      - (III) the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark, as that term is defined in section 34(d) of the Lanham Act or section 2320 of title 18, United States Code; or

SOPA content

- **SEC. 104. IMMUNITY FOR TAKING VOLUNTARY ACTION AGAINST SITES DEDICATED TO THEFT OF U.S. PROPERTY.**

  No cause of action shall lie in any Federal or State court or administrative agency against, no person may rely in any claim or cause of action against, and no liability for damages to any person shall be granted against, a service provider, payment network provider, Internet advertising service, advertiser, Internet search engine, domain name registry, or domain name registrar for taking any action described in section 102(c)(2), section 103(d)(2), or section 103(b) with respect to an Internet site, or otherwise voluntarily blocking access to or ending financial affiliation with an Internet site, in the reasonable belief that

  - (1) the Internet site is a foreign infringing site or is an Internet site dedicated to theft of U.S. property; and
  - (2) the action is consistent with the entity's terms of service or other contractual rights.

OUTLOOK

- Uncertainty - possibly lowering the progress of online activities
- It has an anti SME trend
- It will heat up agian the ICAN debate
- It brings legal aspects cross borders cross juristiction into the debate

EMOTINALLY HIGH UP

A Vibrant Political Debate on ACTA Sparks at the EU Parliament

Submitted on 29 Feb 2012 - 09:38
Tags: ACTA, De Gucht, press release

Printer-friendly version | Send to friend

Brussels, February 29th, 2012 – **The European Parliament may be adopting a strong political line on the Anti-Counterfeiting Trade Agreement (ACTA), despite the EU Commission's attempt to buy time and defuse the debate. Due to the referral of ACTA to the EU Court of Justice, the final vote paving the way for its ratification will be delayed. This will give the EU Parliament time to build up a clear stance on the issues raised by this dangerous trade agreement, do in-depth research and impact assessments, and hopefully define guidelines for a better and fair copyright regime. Citizens must remain mobilized, as they will have many opportunities to weigh in this open process.**

On February 28th, David Martin, the rapporteur for ACTA in the International Trade committee ("INTA") held a press conference marking the beginning of an important "ACTA week" in the European Parliament. Reacting to the Commission's attempt to defuse the political debate by referring ACTA to the EU Court of Justice, he affirmed that the EU Parliament will continue its work towards building a political position on key questions (impact of ACTA on fundamental rights, a free Internet, innovation, supply of generic medicines, etc.). Answers to these questions may lead the European Parliament to reject ACTA, by refusing to give its consent to ratification.

MEP David Martin and EU Commissioner for Trade Karel De Gucht, a few months ago.

- http://www.big-screen.de/deutsch/pages/news/allgemeine-news/2012_01_18_8212_zahlreiche-webseiten-beteiligen-sich-am-sopa-protest.php

- https://www.laquadrature.net//acta