Asia-Pacific
Economic Cooperation

2021/CTI/WKSP2/013
Day 2 Session 1

Domestic Approaches of Marks Protection in Digital Trade: Takeaways from the Uniform Domain-Name Dispute-Resolution Policy Experience

Submitted by: World Intellectual Property Organization

NEW ZEALAND
APEC 2021
ASIA-PACIFIC ECONOMIC COOPERATION 2021

Workshop on Protection of Intellectual Property Rights in Digital Content Trade
20-21 April 2021

WIPO | ADR
Arbitration and Mediation Center

[Domestic approaches of marks protection in digital trade]
Takeaways from the UDRP experience

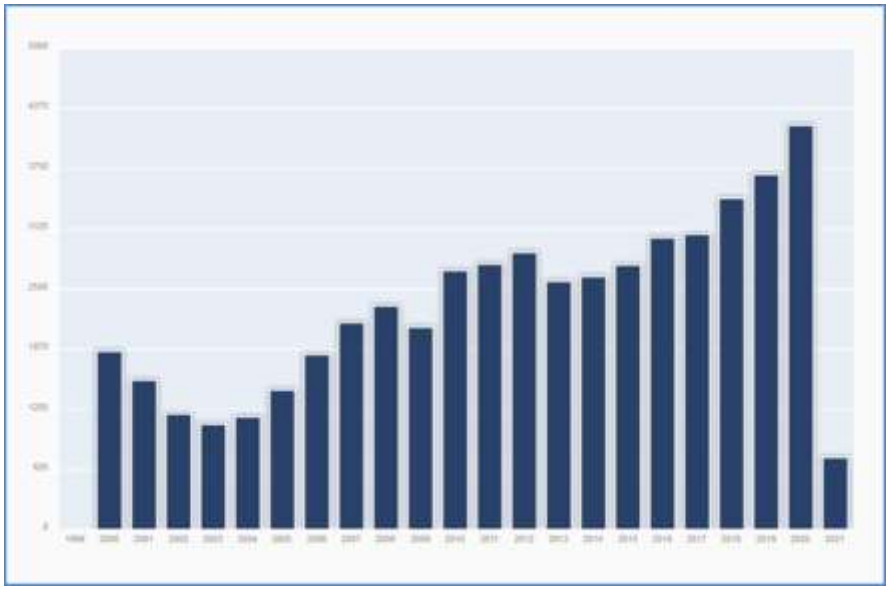
APEC Virtual Workshop: Protection of IP Rights in Digital Content Trade
April 20-21, 2021

Brian Beckham, World Intellectual Property Organization

UDRP case filing snapshot

- Surge during COVID-19 crisis: abuses in the biotech/pharma, Internet/IT, banking/finance, and events-related categories

  - <sanofi-vaccine.com>
  - <pfizer-biontech.com>
  - <belfius-quarantaine.com>
  - <virgincovid19team.com>
  - <coronavirusgilead.com>
  - <hmrc-refund-covid19.com>
  - <verizonwireless-covid-19.net>
  - <tokyo2021.cn>
  - <plaquenil.club>



- *www.wipo.int/amc/en/news/2020/cybersquatting_covid19.html*

WIPO | ADR
Arbitration and Mediation Center

Trademarks protect consumers online

- INTA
  - *"Trademarks promote freedom of choice and enable consumers to make quick, confident, and safe purchasing decisions."*

[from prior handout slide]

- Protecting brands online helps mitigate consumer confusion and related harms, curb abusive practices, and provide a stable platform for global economic growth
  - The UDRP is a vital contribution to these collective benefits

Addressing trademark abuse in the DNS

- Bad actors in the DNS target brands and defraud unsuspecting consumers
- The **global nature of the Internet requires global solutions** to combat such practices
- At the request of the US with WIPO Member States' approval, to address bad actors engaged in "cybersquatting" in **1999 WIPO designed the UDRP**
- As a global dispute resolution mechanism, the UDRP resolves domain name disputes **without a need for expensive court litigation**
- **WIPO has managed over 50,000 UDRP cases** for stakeholders from all over the world

WIPO | ADR
Arbitration and Mediation Center

Further UDRP benefits

- Trademark-abusive domain names are also used to perpetuate phishing, fraud, counterfeiting, and employment scams, to distribute malware, or for illegal prescription drugs

- Beyond assisting brand owners in addressing such abuses of their trademarks online, the UDRP:

  - Minimizes burdens on domestic courts
  - Promotes trust, and protects consumers
  - Provides predictability for the domain investment aftermarket
  - Provides an outsourced safe harbor for ICANN Contracted Parties: keeping them out of cybersquatting disputes and courts

- A globally-recognized best practice, the UDRP is the basis for over 75 ccTLD dispute resolution policies in all regions

WIPO Briefing Note for the ICANN Governmental Advisory Committee:

Continued UDRP stability benefits all ICANN stakeholders

Protecting brands online helps to mitigate consumer confusion and related harm, curb abusive practices, and provide a stable platform for global economic growth. In the DNS, the UDRP (the Uniform Domain Name Dispute Resolution Policy) is a vital contribution to these collective benefits.

The Internet and DNS significantly contribute to the global economy

With 3.2 billion (and growing) estimated Internet users globally, the digital economy increasingly contributes to GDP and promotes innovation and job creation.

- In 2016 brands spent nearly USD 500 billion on advertising globally[1]
- By 2016 the Internet economy of the G-20 was expected to reach USD 4.2 trillion (5.3% of GDP)[2]
- High- and medium-Web SMEs experience significant revenue growth, and generate more jobs[3]

Addressing trademark-abusive conduct in the DNS

Even for all of its positive attributes, as with much public technology, the Internet and DNS also bring their share of bad actors. Many of these bad actors target brands and defraud unsuspecting consumers. To combat such practices, the global nature of the Internet requires global solutions.

At the request of the United States Government with WIPO Member States' approval, to address bad actors engaged in "cybersquatting" in 1999 WIPO designed the UDRP. As a global dispute resolution mechanism, the UDRP resolves domain name disputes without a need for expensive court litigation. Through 2017, WIPO has managed almost 40,000 cases with parties from 175 countries.

In many cases, trademark-abusive domain names are also used to perpetuate phishing, fraud, counterfeiting, and employment scams, to distribute malware, or for illegal prescription drugs.

Further UDRP benefits

Beyond assisting brand owners in addressing abuse of their trademarks online, the UDRP

- Minimizes burdens on national courts
- Promotes trust, and protects consumers
- Provides predictability for the domain investment aftermarket
- Provides a safe harbor for ICANN Contracted Parties: keeping them out of cybersquatting disputes and courts

As a globally-recognized best practice, and part of WIPO's capacity-building, the UDRP is also the basis for over 75 ccTLD dispute resolution policies in all regions.

WIPO as the UDRP's recognized steward

Operating on a not-for-profit institutional basis, WIPO invests in training for Panelists and Parties and produces a globally-used Jurisprudential Overview covering thousands of cases over time.

[1] MAGNA Global Advertising Forecast, www.magnaglobal.com/wp-content/uploads/2016/12/MAGNA-December-Global-Forecast-Update-Press-Release.pdf.
[2] BCG Report: The Internet Economy in the G-20. https://www.bcg.com/documents/file100409.pdf.
[3] Id. For example, over a 3-year period in Brazil, 98% of High-Web SMEs added jobs vs 77% for Low-Web SMEs.

WIPO Briefing Note for the ICANN Governmental Advisory Committee:

Continued UDRP stability benefits all ICANN stakeholders

Without such WIPO stewardship, UDRP predictability and DNS stability would be severely undermined.

- WIPO's institutional investment includes a range of further tools, including real-time case statistics and an online searchable Legal Index – both promoting UDRP transparency
- WIPO has initiated e-filing, case language practices, and settlement facilities
    - In support of case language capacity, WIPO as a global provider has managed cases in over 20 languages

Risks to the UDRP inherent in ICANN's structure

ICANN, for institutional reasons, has decided to initiate a PDP to review the UDRP and the related new gTLD mechanism, the URS.

This ICANN process carries a serious risk of undermining the UDRP's effectiveness.

Both institutionally and in practice, ICANN process is weighted towards registration interests.

An expert-driven UDRP review avoids undermining the UDRP's functioning

Achieving a UDRP net-positive would mean ICANN, as a technical body, giving appropriate weight to WIPO input, experience, and expertise.

Having created the UDRP, WIPO through tens of thousands of cases uniquely understands the policy and practical implications of even well-intended UDRP (and URS) "improvements", in substance and in process terms.

With its flexible and forward-looking design, the UDRP remains globally-valued as an up-to-date rights protection tool. Its current design should be preferred to an unwieldy "revised" mechanism that fails in practice.

The ICANN-produced URS is a case study in unwieldy design-by-committee. Serious concerns regarding its efficacy and operational sustainability remain, which are reflected in its underutilization. Without a fully informed process, there is a real risk that the UDRP will go the way of the URS (in which case, regrettably, WIPO would need to carefully examine its continued UDRP investment).

To produce the UDRP in the first place, WIPO provided its UDRP blueprint to ICANN for review and implementation. To consider the future of this unique global dispute resolution mechanism, WIPO would be prepared to provide its expert leadership.

The GAC

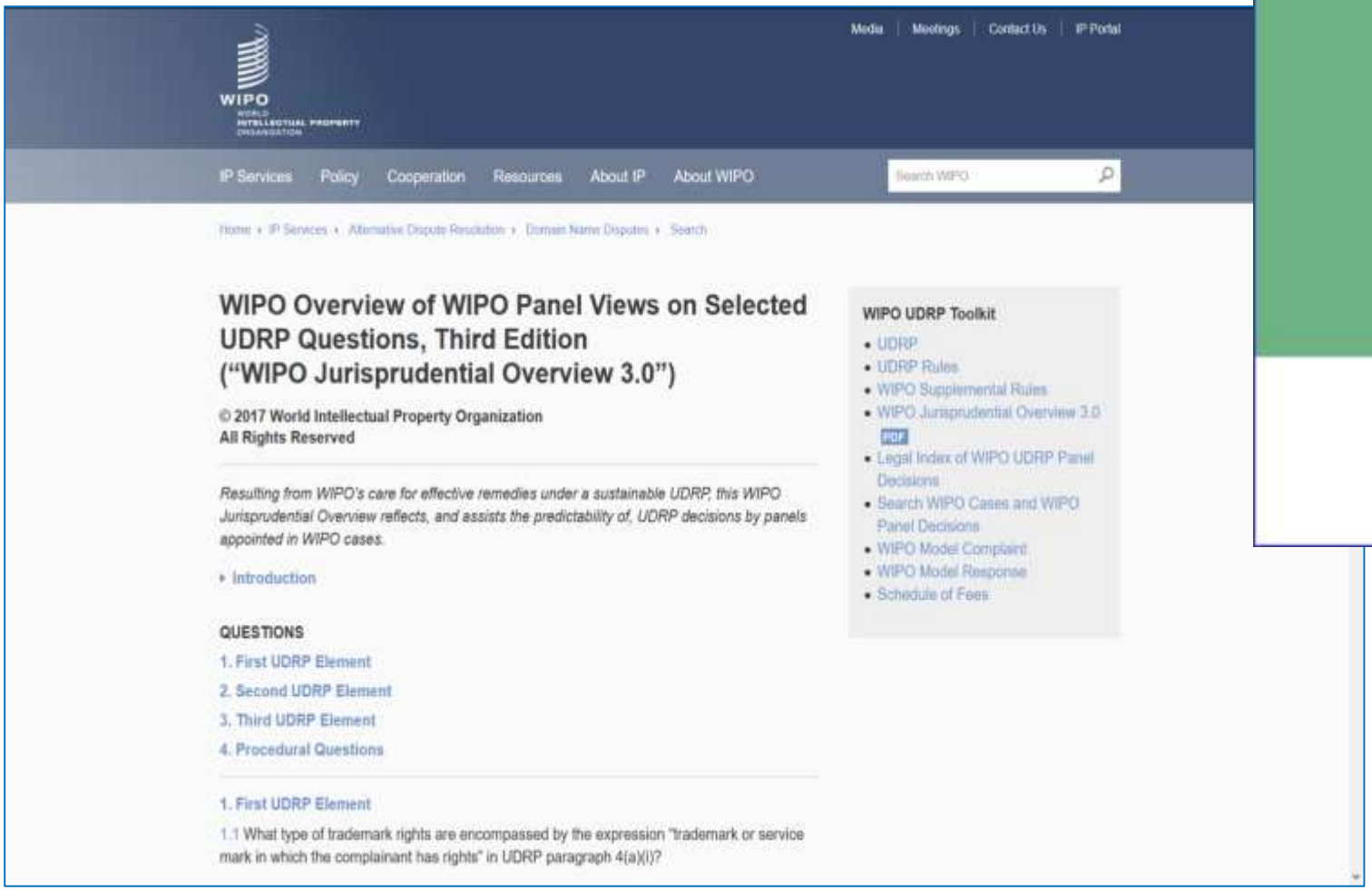
As the digital economy grows, and ICANN considers future new gTLD rounds, the potential for cybersquatting and consumer harm only increases – making continued UDRP stability all the more important. Any responsible ICANN process should use WIPO's unique substantive UDRP expertise and operational experience.

To preserve the UDRP's vital role in tomorrow's digital economy, GAC support for continued UDRP stability is instrumental. Conveying this support to ICANN would enable brand owners and consumers to continue to rely on the UDRP.

Key UDRP elements

- Global: significantly quicker and cheaper than piecemeal and domestic court litigation
- Contractual: decision (transfer) implemented directly by registrars
- Experience: 20+ years of WIPO know-how
- Straightforward (3) legal criteria/defenses
- Predictable: 50,000+ WIPO cases (incl. ccTLDs)
- Free resources: the WIPO Overview

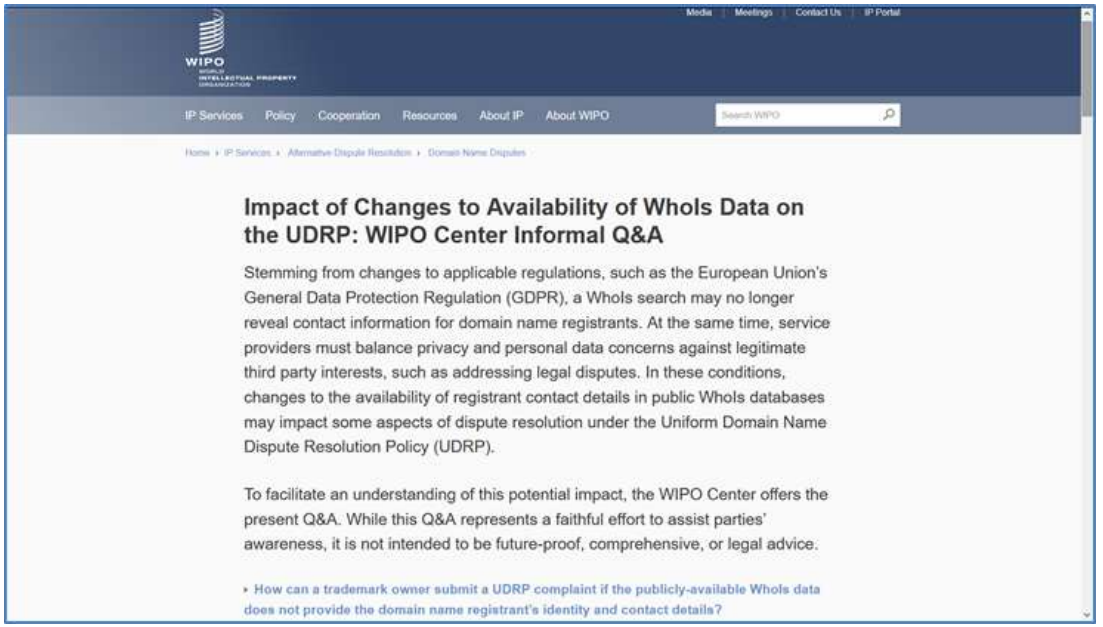
UDRP resources



WIPO | ADR
Arbitration
and Mediation
Center

UDRP resources

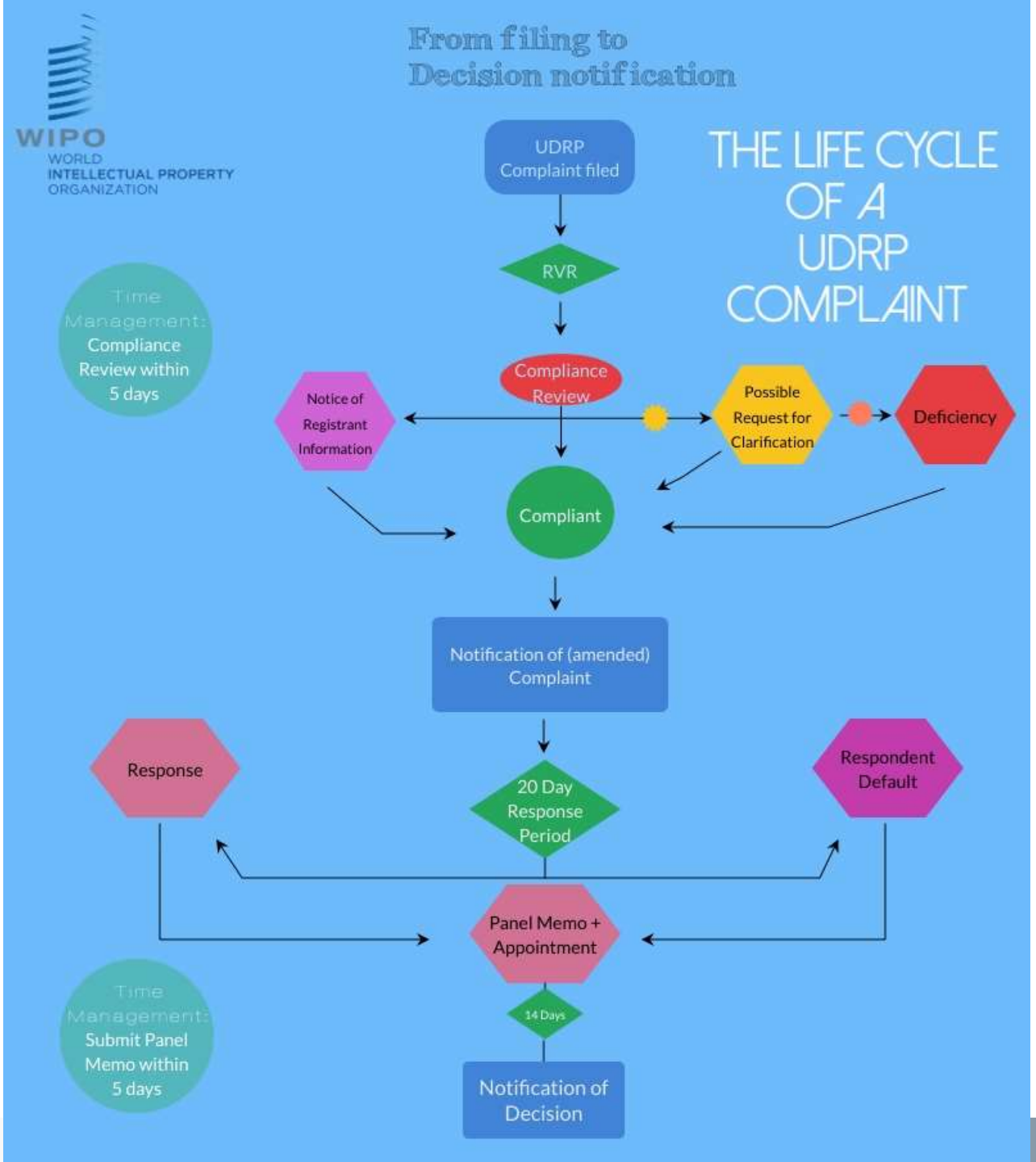
- Access to WhoIs information



WIPO | ADR
Arbitration and Mediation Center

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

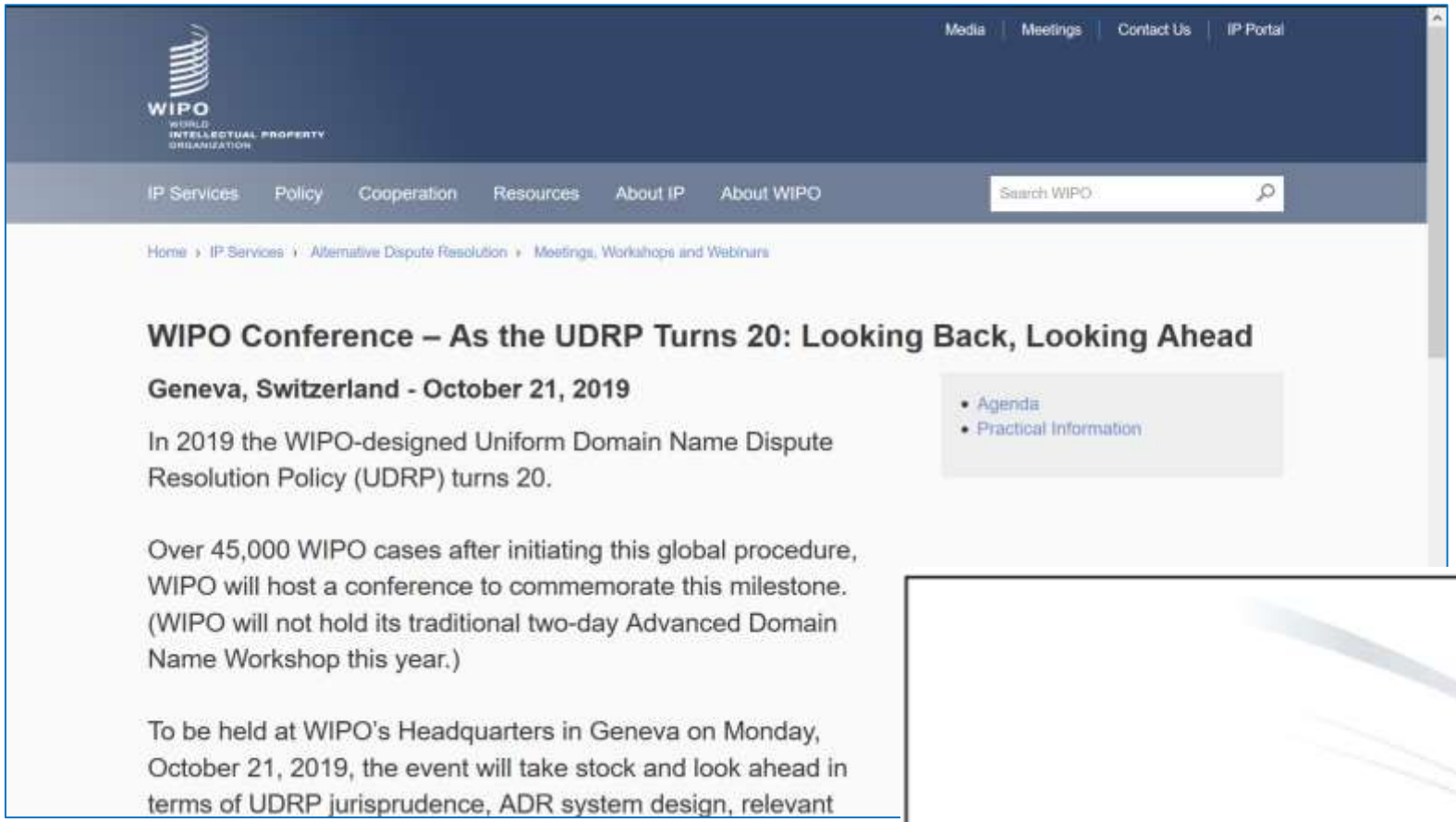
From filing to Decision notification



WIPO | ADR
Arbitration
and Mediation
Center

[Domestic approaches of marks protection in digital trade]
Takeaways from the UDRP experience

- Global UDRP/domestic ccTLDs
- Notice+Takedown
  - DMCA
  - Platform-specific



WIPO
WORLD INTELLECTUAL PROPERTY ORGANIZATION

Media | Meetings | Contact Us | IP Portal

IP Services | Policy | Cooperation | Resources | About IP | About WIPO

Search WIPO

Home › IP Services › Alternative Dispute Resolution › Meetings, Workshops and Webinars

WIPO Conference – As the UDRP Turns 20: Looking Back, Looking Ahead

Geneva, Switzerland - October 21, 2019

- Agenda
- Practical Information

In 2019 the WIPO-designed Uniform Domain Name Dispute Resolution Policy (UDRP) turns 20.

Over 45,000 WIPO cases after initiating this global procedure, WIPO will host a conference to commemorate this milestone. (WIPO will not hold its traditional two-day Advanced Domain Name Workshop this year.)

To be held at WIPO's Headquarters in Geneva on Monday, October 21, 2019, the event will take stock and look ahead in terms of UDRP jurisprudence, ADR system design, relevant

WIPO | ADR
Arbitration and Mediation Center

IP dispute resolution models for platforms

WIPO Conference: As the UDRP turns 20: looking back, looking ahead

Geneva
October 21, 2019

Andrew Christie, Melbourne Law School
Larry Nodine, Ballard Spahr Andrews & Ingersoll, LLP

	UDRP	DMCA	"DMCA auto" / "DMCA plus"
Space	Public: gTLDs (incl. new) ccTLDs	Private: OSPs (Yahoo)	Private: OSPs (Amazon, Google, YouTube, Facebook) Public: new gTLDs (.movie)
Infringed right	TM	Copyright	Copyright, TM, patent, privacy, reputation, …
Criteria	Simplified non-domestic principles	Domestic law	Complex domestic law No law / privatized principles
Decision-maker	Independent (panelists)	OSP (staff)	OSP (automated) Rights-holder (automated)
Remedy	Transfer/cancel domain name	Take-down material	Take-down material Not put-up material
Speed	Months	Days	Seconds
Scale (p.a.)	1,000s	10,000s	100,000,000s
Internal appeal	No	Sort of	Not really
Transparent	Yes	No	Hardly

Intellectual Property Protection Strategies of Online Intermediaries

Christian Borggreen
VP and Head of Office, Computer and Communications Industry Association (CCIA) Europe, Brussels, Belgium

Introduction

- Benefits of online services for users, economy
- The Internet sector makes significant efforts to prevent copyright infringement online, in large part enabled by the prevailing legal framework worldwide: "notice-and-action" ("notice-and-takedown" in the U.S.)
- In addition to copyright compliance, services remove content that infringes trademark rights, or violates community guidelines

Notice-and-Action/ Notice-and-Takedown

What is notice-and-action/notice-and-takedown?

- Follows U.S. Digital Millennium Copyright Act (DMCA Section 512) and EU E-Commerce Directive (Articles 12-15)
- Widely implemented globally
- Common in free trade agreements

WIPO | ADR
Arbitration and Mediation Center

"DMCA plus" – Voluntary Efforts Fostered by Notice-and-Takedown

What is "DMCA plus"?

- Many services have invested in IP protection processes and tools beyond what is required by law, *e.g.*:
  - 'Trusted user' programs that facilitate bulk notice sending for 'trusted' senders and fast-track takedown
  - Direct access to back-end systems, so senders can remove content proactively
- "DMCA plus" systems provide value when deployed voluntarily by firms that have the resources to do so competently

Computer & Communications Industry Association

CCIANET.ORG

Examples

Voluntary IP protection programs and tools include:

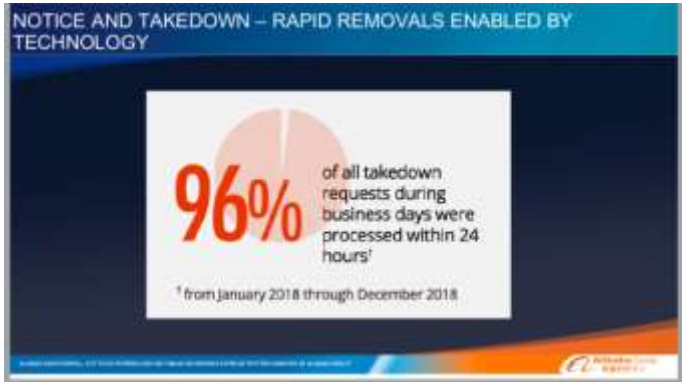
- Amazon Brand Registry
- eBay Verified Rights Owner Program
- Facebook Rights Manager
- Facebook Commerce & Ads IP Tool
- Google Search Trusted Copyright Removal Program
- YouTube Content ID

Computer & Communications Industry Association

CCIANET.ORG

Notice+Takedown: big and fast

Alibaba Group's Achievements in Intellectual Property Protection



Protecting IP on Facebook and Instagram

Turnaround Time

- Reports are regularly handled within one day
- Often, reports are processed within hours or even minutes
- Copyright: < 2 hours
- Counterfeit: < 3 hours
- Trademark: < 8 hours

IP Transparency Report

- July-December 2018 for Facebook and Instagram:
  - 2.6 million pieces of content removed based on 512,000 copyright reports
  - 216,000 pieces of content removed based on 81,000 trademark reports
  - 782,000 pieces of content removed based on 63,000 counterfeit reports

Google

Protecting Copyright in Google Search

4 billion pages

removed from our index

for copyright infringement

1.7 billion

ads removed from our system

for infringement of our policies

in 2016

Instagram: Keyword Filters & Additional Measures

- Working with trusted rights holders, Instagram has implemented proactive measures to reduce the visibility and prevalence of potential counterfeits:
  - Hashtags containing certain combinations of brand names and replica keywords are blocked from Instagram search – e.g., #<brand><keyword>
  - Instagram posts that contain combinations of certain brand names and replica keywords (in text, separate hashtags, or combination of text and hashtags) are hidden from search – e.g., #<brand> #<keyword>
  - Instagram posts whose captions contain four or more brand-name hashtags are hidden from search – e.g., #<brand1> #<brand2> #<brand3> #<brand4>
  - Automation detects repeated use of the same phone number containing the Chinese country code (86) in bios across multiple accounts

Domain Registries: “Trusted Notifiers”

MPA

MARCH 6, 2017

A year has passed since the MPAA teamed up with Donuts Inc., the largest operator of new domain name extensions, to establish a Trusted Notifier Program to ensure that websites using domains registered with Donuts are not engaged in large-scale piracy. Following this unprecedented announcement, the MPAA also solidified a similar partnership with Radix, the first such agreement with a registry based outside the United States.

“Of the eleven on which action was taken, each represented a clear violation of law—the key tenet of a referral,” Donuts explained. “All were clearly and solely dedicated to pervasive illegal streaming of television and movie content. In a reflection of the further damage these types of sites can impart on Internet users, malware was detected on one of the sites.”

Donuts continued: “There has been concern on the part of some in the industry about this type of arrangement—namely, that it represented a ‘slippery slope’ toward inappropriate content control, or that hundreds of domain names would be snatched away from rightful registrants. To the contrary, however, and in line with the previously published characteristics of a Trusted Notifier Program, a mere handful of names have been impacted, and only those that clearly were devoted to illegal activity. And to Donuts’ knowledge, in no case did the registrant contest the suspension or seek reinstatement of the domain.”

Some Notice+Takedown drawbacks

- Substance: overbroad and imprecise notices
- Scope: automation casting too wide a net (false positives)
- Lack of meaningful counter notices
- No neutral decision makers
- Lack of transparency (no published decisions)
- ***Overall*: still seen as too much of a black box**

Policy research on automation consequences of Notice+Takedown

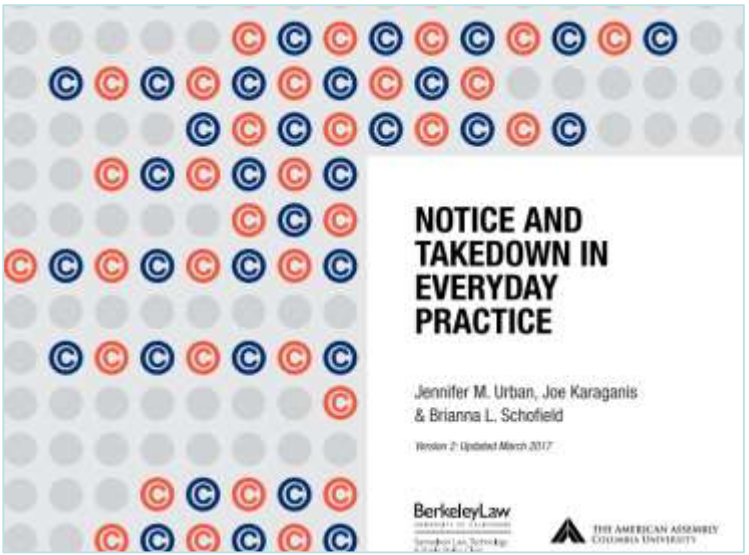
The Takedown Project

Collaborative research on Internet takedown law and policy

Home About Affiliated Researchers Projects Resources

Welcome

The Takedown Project is a collaborative effort housed at UC-Berkeley School of Law and the American Assembly to study notice and takedown procedures. Researchers in the US, Europe, and other countries are working collaboratively to understand this fundamental regulatory system for global online speech.



"Who watches the watchmen?" An Empirical Analysis of Errors in DMCA Takedown Notices

An Empirical Study of DMCA Takedown Notices

Daniel Seng†

WIPO | ADR
Arbitration and Mediation Center

Overbroad and imprecise notices

2. Questions of Accuracy and Substantive Judgment

Overall, the general picture that emerged from the Lumen data—an overwhelming focus on Google Web Search, a high level of automation and third-party notice sending, heavy use by major entertainment companies, and a focus on file sharing and torrent sites—still leaves open the question of how accurate these efforts are. As we observed in Study 1, for some senders and for DMCA Auto and DMCA Plus OSPs, notice and takedown has evolved from a low-volume process based on human decision-making to a process dominated by automated systems capable of sending and processing massive numbers of requests. As the scale of the process increases and significant human review becomes impossible, the integrity of the process comes to depend increasingly on the accuracy of these systems. So how accurate are automated notices? To answer this question for our dataset, we examined the substance of each takedown request and its underlying claim of infringement.

- One in twenty-five of the takedown requests (4.2%) were fundamentally flawed because they targeted content that clearly did not match the identified infringed work. This extrapolates to approximately 4.5 million requests[246] suffering from this problem across the entire six-month dataset.

We found reason to be concerned when human review is replaced with a high degree of automation. The automated notices we examined in Study 2 were, in the main, sent by sophisticated rightsholders (or their agents) with a strong knowledge of copyright law, yet nearly a third of the notices raised questions about their validity, and one in twenty-five apparently targeted the wrong material entirely.

Fair Use implications

About one in fifteen (6.6%) requests had at least one characteristic that likely weighs favorably toward fair use. These requests predominantly targeted such potential fair uses as mashups or remixes, or links to search results pages including mashups or

About 1 in 15 (6.6%) of requests were flagged with characteristics that weigh favorably toward fair use.

weigh favorably toward fair use, suggesting that further review could reveal a fair use defense. Over half of these were requests to take down allegedly infringing material on news sites. Others included requests where the allegedly infringing material was apparently being used for educational purposes, such as a scientific photograph of bacteria under a

We could not do a full fair use analysis, and focused on characteristics that reviewers could observe and record relatively easily. The final merit of any potential fair use claims within this set will vary. Our goal was to observe whether automated systems appeared to generate any significant number of notices for which more contextualized human review is needed to check for fair use. It appears that they do: around 7 million notices out of the full 108.3 million can be expected to present these issues.[282]

Lack of meaningful counter notices

4. Counter Notices: Inadequate and Infrequently Used

By its structure, section 512 mostly leaves due process for targets to the privately adjudicated notice-and-takedown process.[123] The main mechanism is the DMCA's "counter notice."[124]

content stays down pending the outcome.[127] If no action is taken within the ten days, the OSP may restore the content and retain safe harbor protection.[128] While some rightsholders expressed some faith in the counter notice process, OSPs mostly considered it a dead letter—impractical and rarely used. All OSPs and at least one rightsholder agreed that the counter notice procedure's practical ability to protect targets is limited.[129] All agreed that the process has major deficiencies.

Second, by all accounts, the actual use of counter notices is extremely infrequent. Only one respondent among both service providers and rightsholders reported receiving more than a handful per year. Many—including some large services handling thousands of notices per year—reported receiving none.

In the end, counter notice and putback give the appearance of due process for targets without the necessary components of definite notice of the claimed transgression, a reasonably exercisable ability to respond (preferably before action is taken), and an unbiased adjudicator.[318] In the recommendations section below, we build on others' efforts to offer suggestions for improving this situation. Moreover, further expansion of the notice

Lack of transparency

Despite the commonalities in OSPs' experiences, they uniformly reported having little knowledge of other service providers' notice and takedown practices. Knowledge about how services manage notice and takedown across the Internet sector remains remarkably limited.

Several OSPs told us that this lack of transparency leaves them in the dark about how others manage the DMCA's various ambiguities, at times leading them to make decisions and set policies conservatively. In general, OSPs agreed that more information would support good internal practices and potentially improve public relations by anchoring commitments to

Given Notice+Takedown drawbacks, the Challenge:

- Size and scale of Internet abuse is forcing reliance on blunt rough tool: automated/imprecise Notice+Takedown
- **A core question:** how to give (procedural and substantive) meaning and transparency/fairness to counter notice
- **A proposed solution:** UDRP-like procedures cannot address billions of abuses, but…
  - ***for a certain path in the enforcement chain*** could be made available

[Domestic approaches of marks protection in digital trade]
Takeaways from the UDRP experience

- Procedural clarity
  - [beyond (i) intake, (ii) result]
- Clarity on substantive criteria/their application
- Human (non-automated) assessment of counter-notices (“appeals”)
- Neutral (independent) assessor
  - Appointed by an independent body (e.g., WIPO in the UDRP)
- Publication of reasoned decisions
  - Searchable/precedential, not necessarily binding