Internet Law: Class 3

Professor Marketa Trimble

Class 3 (Monday, 19 April 2021)

1. Internet Domain Names (2)
2. Immunity and liability of internet service providers
3. Notice and takedown under the DMCA
4. DSM Directive
5. Immunity from suit under the CDA
6. Blocking orders

A list of all top-level domains:

https://data.iana.org/TLD/tlds-alpha-by-domain.txt

TLD startup information:

https://newgtlds.icann.org/en/program-status/sunrise-claims-periods

ICANN Uniform Domain-Name Dispute-Resolution Policy

- Disputes:
  - (1) The domain name "is identical or confusingly similar to a trademark or service mark in which the complainant has rights;" and
  - (2) The Registrant has "no rights or legitimate interests in respect of the domain name;" and
  - (3) The Registrant's "domain name has been registered and is being used in bad faith."

ICANN Dispute Resolution v. Court Proceedings

- "Availability of Court Proceedings" under the ICANN Policy
- **U.S. provisions**
  - The Anti-cybersquatting Consumer Protection Act, 15 USC 1125(d) (1999)
    - https://www.law.cornell.edu/uscode/text/15/1125
  - The Reverse Domain Name Hijacking provision, **15 U.S.C. §1114(2)(D)(v)**
    - https://www.law.cornell.edu/uscode/text/15/1114

Barcelona.com v. Barcelona

- Why did the City want barcelona.com?
- Why didn't the City obtain barcelona.es or barcelona.eu at the time of the dispute?
- ICANN UDRP proceeding outcome
- Lawsuit in the U.S.
- Jurisdiction of the U.S. court over the City of Barcelona
- The reverse domain name hijacking provision
- Legality of the domain name registration under the Lanham Act, 15 USC 1125(d)
- Which law governs whether a trademark exists or not?
  - Spanish law v. U.S. law v. the law of the dispute resolution provider v. the law of the registry?

.CAT Registry Agreement, Specification 12

"The TLD will be established to serve the needs of the Catalan Linguistic and Cultural Community on the Internet (the "Community"). The Community consists of those who use the Catalan language for their online communications, and/or promote the different aspects of Catalan culture online, and/or want to specifically address their online communications to that Community."

Examples:

- "Universities, schools, research institutions and other academic entities that use Catalan in their academic activities or teach/promote aspects of Catalan culture
- public or private entities whose aim is promoting the Catalan culture …
- media using the Catalan language for their communications
- individuals, groups, businesses, organizations, entities or initiatives, however constituted, carrying online communications in Catalan …"

Choice of law was always present in UDRP cases, to some extent.

- Disagreements exist among UDRP panelists about the role, if any, that **national law** should play in UDRP cases.
- National law is applied to determine the **existence, validity, and ownership of trademarks**.
  - Barcelona.com showed that choice of law does matter in UDRP cases.
- Some panels have applied national law to determine **other issues** in UDRP cases.
  - E.g., non-commercial fair uses of trademarks.
- The **methods** through which UDRP panels select applicable national law have varied.

- The registries for some top-level domains have adapted the text of the UDRP or have adopted a different dispute resolution policy to give **preference to national or local rights**.
  - Listing preferred national rights
    - E.g., .br (Brazil), .eu (European Union), .ie (Ireland), .se (Sweden)
  - Listing applicable law
    - E.g., .de (Germany), .dk (Denmark), .eu (European Union)

Internet Intermediaries

Who Are Internet Intermediaries?

- Entities that facilitate activities on the internet
  - Internet service providers (ISPs)
  - Other intermediaries (e.g., payment processors)

DMCA (Digital Millennium Copyright Act), 17 USC 512

"…[T]he term "service provider" means an entity offering the **transmission, routing, or providing of connections for digital online communications**, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." 17 USC 512(k)(1)(A)

(a) Transitory communications (e.g., telephone companies)

(b) Caching

(c) Information storage (e.g., eBay, YouTube)

(d) Information location tools (e.g., Google, Yahoo)

Internet Intermediaries

Information service providers?

Utility services?

Common carriers?

ISP Liability

U.S. defamation laws:

Publishers – are responsible for content by others

Distributors – are subject to liability if they know or have reason to know of the defamatory character of content published by others

Conduits – are not liable for content published by others, even if the conduits are aware of the content

Restatement (Second) of Torts §581 (1977)

47 USC 230 (Communications Decency Act, adopted in 1996)

(1) TREATMENT OF PUBLISHER OR SPEAKER

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) CIVIL LIABILITY

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

47 USC 230(c) PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL

(1) TREATMENT OF PUBLISHER OR SPEAKER

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997)

- Mere conduits, or distributors, are subject to a different standard of liability than publishers
- "The simple fact of notice surely cannot transform one from an original publisher to a distributor in the eyes of the law. To the contrary, once a computer service provider receives notice of a potentially defamatory posting, it is thrust into the role of a traditional publisher."

47 USC 230(c) PROTECTION FOR "GOOD SAMARITAN" BLOCKING AND SCREENING OF OFFENSIVE MATERIAL

(2) CIVIL LIABILITY
No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)

DIGITAL MILLENNIUM COPYRIGHT ACT

- Adopted in 1998
- Section 512
  - Liability of ISPs ("OSPs")
- Sections 1201 ff.
  - Protection of digital rights management

§512 (k)

(k) Definitions.—

(1) Service provider. —

(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

§512 (i)

(i) Conditions for Eligibility.—

(1) Accommodation of technology. — The limitations on liability established by this section shall apply to a service provider only if the service provider —

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

17 USC 512 (Digital Millennium Copyright Act, adopted in 1998)

(a) Transitory communications (e.g., telephone companies)

(b) Caching

(c) Information storage (e.g., eBay, YouTube)

(d) Information location tool (e.g., Google, Yahoo)

Notice & takedown

17 USC 512 (Digital Millennium Copyright Act, adopted in 1998)

1) Notification
2) Removal by ISP
3) ISP notifies the subscriber
4) Subscriber sends a counter-notification
5) ISP provides a copy of the counter-notification to the © owner
6) In 10 – 14 days following the receipt of the counter-notification, either the ISP replaces the removed material, or the rights owner files an action in court seeking to restrain the subscriber

§512(c)

(c) Information Residing on Systems or Networks at Direction of Users.—
(1) In general. — A service provider shall not be liable … for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -

(A)(i) does not have actual knowledge …;
(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

17 USC 512 (Digital Millennium Copyright Act, adopted in 1998)

Problems

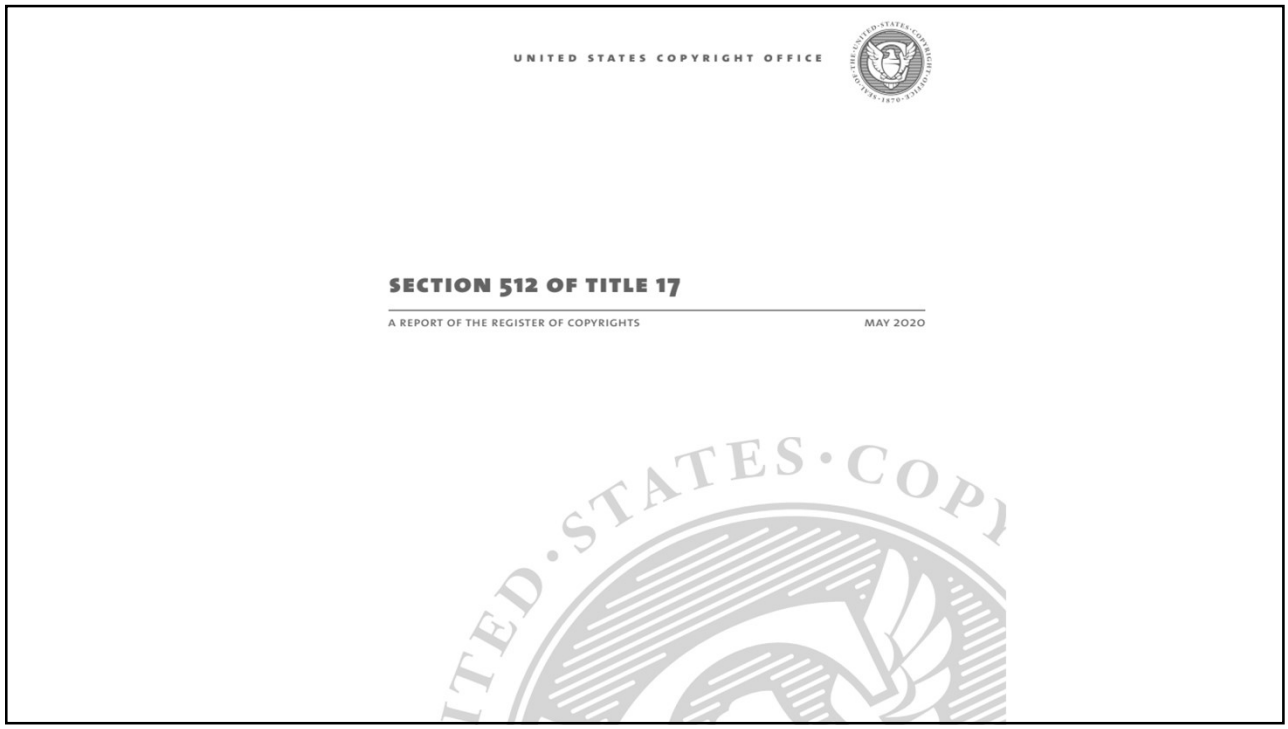
- Notifications are misused to chill speech
  - Lumen Database (formerly "Chilling Effects")
    - https://lumendatabase.org/
  - Google Transparency Report
    - https://transparencyreport.google.com/copyright/overview
- Although the periods in the DMCA are short, they may still be sufficient to effectively prevent certain speech
- A DMCA notification may establish personal jurisdiction over the copyright owner in the place of the alleged infringer (which the alleged infringer may use to file a declaratory judgment suit against the copyright owner)

LENZ V. UNIVERSAL

- The copyright owner "must consider the existence of fair use before sending a takedown notification under § 512(c)."
- The copyright owner must form a subjective good faith belief that the allegedly infringing material does not constitute fair use.
- Good faith belief is to be assessed based on actual knowledge.
- "[T]he willful blindness may be used to determine whether a copyright holder knowingly materially misrepresented that it held a good faith belief that the offending activity was not a fair use."
- "[The plaintiff] did not show that the defendants subjectively believed there was a high probability that the video constituted fair use."

IMPACT OF DMCA S. 512

- E.g., Google has received takedown notices for more than 5 billion URLs
  Transparency Report, Google,
  https://transparencyreport.google.com/copyright/overview, 30 March 2021
- Since 2002, "Chilling Effects"/"Lumen" database,
  https://www.lumendatabase.org/
- Since 2011, Google's "Transparency Report"
- J. Urban et al., *Notice and Takedown in Everyday Practice*, v. 2, revised in March 2017
  https://dx.doi.org/10.2139/ssrn.2755628
- U.S. Copyright Office's "Section 512 Study," 21 May 2020
  https://www.copyright.gov/policy/section512/section-512-full-report.pdf



Section 512 of Title 17: A Report of the Register of Copyrights, U.S. Copyright Office, May 2020

"The Copyright Office concludes that the balance Congress intended when it established the section 512 safe harbor system is askew. … While OSPs, supported in many aspects by user advocacy groups, report satisfaction with the current operation of the safe harbors, that view is not shared by the other intended beneficiaries of the section 512 system, including authors, creators, and rightsholders of all sorts and sizes."

(p. 197)

Section 512 Report Recommendations (1)

- Clarify eligibility
  - "by reason of storage"
  - "temporariness"

- Repeat infringer policy
  - "a clear, documented, and publicly available repeat infringer policy"
  - "what constitutes "appropriate circumstances" for termination of a user's account based upon repeated acts of infringement, and whether such circumstances can ever arise in the absence of a formal takedown notice from a rightsholder"

Section 512 Report Recommendations (2)

- Knowledge requirement
  - Clarification of the distinction between actual and red flag knowledge
  - Clarification of the relationship between the section on the intent to avoid the imposition of a duty to monitor and the section on knowledge requirements
  - Clarification of the willful blindness standard

- Details of a takedown notice
  - Clarify what is "information reasonably sufficient … to locate" the infringing material

- Knowing misrepresentation and abusive notices or counter-notices
  - Increased penalties

Section 512 Report Recommendations (3)

- Copyright owner's fair use analysis
  - Monitor the impact of the *Lenz* decision
- Notice requirements
  - Move to a regulatory process to make setting rules more flexible
- Alternative dispute resolution
  - Explore ADR as an option to address time frames
- Other proposals

ISPs as Enforcers of Rights

- ISPs may be used to block access to infringing content
  - To **remove** content from the internet (hosting ISPs, domain name ISPs)
  - To **de-list** content from the internet (e.g., from Google's search results)
  - To **block** users' access to content

EU E-Commerce Directive (2000/31/EC)

- Safe harbor for internet service providers:
- Mere conduit (Article 12)
- Caching (Article 13)
- Hosting (Article 14)
- No obligation to monitor

Scarlet Extended v. Société Belge (SABAM)

- CJEU, 2011
- SABAM requested an order "requiring Scarlet to bring … infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software without the permission of the rightholders"
- Protection of fundamental rights
  - Copyright (rights holder)
  - Freedom to conduct business (ISPs)
  - Right to protection of personal data (customers)
  - Freedom to receive and impart information (customers)

Scarlet Extended v. Société Belge (SABAM)

- EU law "…preclud[es] an injunction made against an internet service provider which requires it to install a system for filtering
  - all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;
  - which applies indiscriminately to all its customers;
  - as a preventive measure;
  - exclusively at its expense; and
  - for an unlimited period,

  which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files the sharing of which infringes copyright."

UPC Telekabel v. Constantin Film Verleih

- CJEU, 2014
- Injunction for UPC to block access by customers to infringer's website as regards the copyright owners' works (par. 11)
- Rightholders may apply for an injunction against intermediaries whose services are used by a third party to infringe their copyrights (par. 26)
- Is UPC an "intermediary" covered by Article 8(3) of EU Directive 2001/29 (the Info Soc Directive)? (pars. 30 – 40)
  - How is UPC different from Scarlet in this context?
  - Is a relation between the infringer and the ISP necessary?

UPC Telekabel v. Constantin Film Verleih

- The design of the injunction must respect the protection of fundamental rights
  - Copyright (rights holder) (pars. 61 – 63)
  - Freedom to conduct business (ISPs) (pars. 49 – 54)
  - Freedom to receive and impart information (customers) (pars. 55 – 57)

Directive 2019/790 on Copyright in the Digital Single Market

Article 17: Use of protected content by online content-sharing service providers

- A content-sharing service performs an act of communication to the public (or making available to the public)
- Must obtain an authorization from the rightholders
- Without an authorization the service provider is liable unless
  - Best efforts to obtain authorization,
  - Best efforts "to ensure the unavilability" if rightholders provide "the relevant and necessary information," and
  - Upon a notice disable access to the notified works
- Must establish "an effective and expeditious complaint and redress mechanism"

Directive 2019/790 on Copyright in the Digital Single Market

- Special provision for small providers
- Exceptions for quotation, criticism, review, parody, …
- No general monitoring obligation
- Transposition deadline: June 7, 2021

Territorial Scope of ISP Measures

- **EU "right to be forgotten"**
  - Google initially de-listed results only from national versions of its website (e.g., .es), but eventually decided to geoblock users and de-list results from all versions of its website that were accessible from a given country
    - Fleischer, P., "Adapting Our Approach to the European Right to Be Forgotten," March 4, 2016, http://googlepolicyeurope.blogspot.com/2016/03/adapting-our-approach-to-european-right.html
  - French authorities requested a global removal
    - Fioretti, J., "France Fines Google over "Right to Be Forgotten," Reuters, March 24, 2016, http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX

Equustek Solutions v. Google

- Supreme Court of Canada, 2017
- Equustek v. Datalink lawsuit
- 1992 request that Google de-list Datalink's website
- 1992-1993 Google's de-listing of Datalinks webpages

Equustek Solutions v. Google

- A question of the territorial scope of the order
  - [Google acted voluntarily as far as google.ca]
- International comity?
- Google's freedom of expression?
- Inconvenience to Google?
- Temporary or permanent relief?
- Effectiveness of the remedy?

Google v. Equustek

- **U.S. District Court for the District of Northern District of California, 2017**
  - Preliminary injunction issued in November 2017 (permanent injunction in December 2017)
  - Canadian judgment unenforceable
- **Supreme Court of British Columbia, April 2018**
  - Google's motion to bar or set aside the global injunction dismissed
  - "The U.S. decision does not establish that the injunction requires Google to violate American law."
  - "Google has not demonstrated that the injunction violates core American values."
  - "The effect of the U.S. order is that no action can be taken against Google to enforce the injunction in U.S. courts. That does not restrict the ability of this Court to protect the integrity of its own process through orders directed to parties over whom it has personal jurisdiction."

Glawischnig-Piesczek v. Facebook

- Interim order - Facebook disabled access to the post for users connecting from Austria
- A host provider may be the addressee of the injunction under the E-Commerce Directive
- Facebook had knowledge of the illegal information and did not act expeditiously to remove it
- No general obligation to monitor but possibly an obligation to monitor "in a specific case"
  - A different user
  - A somewhat changed message

Glawischnig-Piesczek v. Facebook

- Territorial scope of an injunction under the E-Commerce Directive
- No territorial limitation in the Directive
  - The Directive "does not preclude those injunction measures from producing effects worldwide."
- It is up to the member states to ensure consistency with international law

Glawischnig-Piesczek v. Facebook

- Oberste Gerichtshof (Austria), 4 Ob 36/20b, 30 March 2020

  "In cases of intellectual property right claims (e.g., copyright claims), the scope of the injunction is limited by the principle of territoriality to the protection within the country.

  In cases of other injunctions, there must be a clear statement by the plaintiff is necessary when the plaintiff wants to require protection extending beyond Austria."

  https://www.ogh.gv.at/entscheidungen/entscheidungen-ogh/unterlassungsanordnungen-sind-auch-gegen-internet-provider-zulaessig-grundsaetzlich-aber-auf-den-schutz-im-inland-beschraenkt/

- The injunction based on copyright infringement is limited to Austria because of the territoriality principle
- The injunction based on the personality rights violation is also limited to Austria because the plaintiff provided no explanation as to the territorial scope of the requested injunction

Internet Law: Class 3

Professor Marketa Trimble