Issue 3 / July 2013

SYNTHESIS

REGULAR UPDATE FROM THE INTERNET & JURISDICTION PROJECT

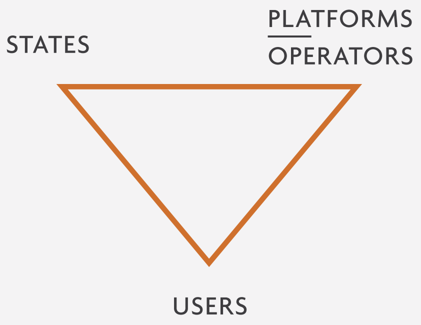
CROSS BORDER DATA FLOWS AND NATIONAL SOVEREIGNTY

Revelations of online surveillance programs with extraterritorial reach trigger demands for accountable and traceable procedures for access to user data on the Internet around the world.

Calls for data sovereignty, strict national compliance and the establishment of local offices and servers of cross-border platforms become louder.

HOW TO ENABLE DIGITAL COEXISTENCE?

More than 2.5 billion users co-exist and interact in shared cross-border online spaces, governed by heterogeneous normative orders: States have vertical legal systems, while online platforms form horizontal orders through their Terms of Service. How to guarantee interoperability between these heterogeneous norms and procedures? How to handle normative collisions?



PROCEDURAL INTERFACES

Existing international cooperation frameworks based on separated national territories do not easily scale up to the transnational nature of the Internet and online interactions. To diffuse tension and avoid fragmentation, there is a growing understanding that fair process frameworks establishing ”procedural interfaces“ between states, Internet platforms or operators, and users need to be developed.

INTERNET & JURISDICTION

A GLOBAL MULTI-STAKEHOLDER DIALOGUE PROCESS

More information about the Internet & Jurisdiction Project at:

www.internetjurisdiction.net

The Internet & Jurisdiction (I&J) Synthesis summarizes the main results of the monitoring activity of the I&J Observatory and the preliminary outcomes of the ongoing global multi-stakeholder dialogue process conducted between January and July 2013. It highlights emerging patterns and is conceptualized to stimulate discussion around a variety of pressing key questions.

Section I ("Global Trends") scrutinizes recent international developments throughout six major issue areas. Section II ("How to Enable Digital Coexistence") addresses the need for appropriate procedures to guarantee the interoperability of diverse public and private normative orders and to handle normative collisions. Finally, Section III "Procedural Frameworks for Interoperability and Fair Process" explores potential building blocks for such procedural interfaces.

IMAGE CREDIT: andrewfhart, hlkljgk

Issue 3/July 2013

SYNTHESIS

1. GLOBAL TRENDS

Surveillance programs with extraterritorial effects, such as PRISM in the US or UK's Tempora, trigger global concerns over privacy, procedural transparency and accountability. As the physical location of servers and operators matters, voices calling for national "data sovereignty" become louder.

COPYRIGHT

REAFFIRMED PROPORTIONALITY NORMS DESPITE SHORTER TAKEDOWN DELAYS

The European Court of Human Rights ruled for the first time on the balance between copyright and freedom of expression[1] and refused[2] an appeal by the founders of the torrent site The Pirate Bay in regards to a conviction for assisting copyright infringement in Sweden. The platform changed its servers' location[3] and ccTLD domain several times[4] to avoid a seizure and operates now under Iceland's ccTLD '.is'.

The pressure for more rapid takedowns increases. A Brazilian court decided[5], in a case involving Google, that operators can be liable for potential damages if they fail to immediately remove plagiarized content upon receiving notifications, without a court order. A new Russian draft law requires website operators to take down potentially infringing content within 72 hours upon notification, otherwise they would be blocked[6]. However, at the same time, an Italian court ruled that blocking an entire platform due to one infringing video would be disproportionate[7].

QUESTIONS

- What do stricter notice and takedown laws mean in terms of fair process and balanced determinations?
- Will copyright takedown procedures influence removal requests of other content (hate speech, defamation etc.)?

Due to public and political criticism for disproportionate copyright enforcement, a new version of CISPA stalls in the US Senate[8], but a six strikes system is implemented in the US jurisdiction[9]. Meanwhile, France removed the Internet cut-off sanction[10] from its own three strikes system Hadopi, just after the first disconnection[11] had been ordered.

FREEDOM OF EXPRESSION

CROSS-BORDER HATE SPEECH AND ONLINE PORN FILTERING

Twitter Inc. ultimately complied with hate speech laws in the French jurisdiction and handed over the user data of the authors of racist tweets with the hashtag "a good Jew" to a French court[12] without a Mutual Legal Assistance Treaty (MLAT) procedure[13]. Its Terms of Service specify that it only reacts to US court orders, but the company is opening offices in France in 2013[14]. The Parisian court also ordered Twitter to implement a notification tool for users in the French jurisdiction. Another demand for user data in connection to the Gezi Park protests is pending in Turkey, where the government demands Twitter to establish a local office[18]. Meanwhile, Facebook agreed to review its global internal determination norms and procedures in regard to requests for removal of hate speech[19], after a wave of protests by women rights groups.

QUESTIONS

- Will requests for the establishment of local offices of cross-border platforms increase?
- How to prevent the blocking of entire platforms for one piece of content?
- How do platforms implement their Terms of Service provisions in view of transnational hate speech?

ISP-based filters on the Internet are on the rise, as Iceland[20], Egypt[21], India[22], Peru[23] and the UK[24] explore or implement measures to limit access to online pornography. The "Innocence of Muslims" YouTube video continues to display the absence of granular takedown procedures: lacking an MLAT with the US, Pakistan blocks the entire YouTube platform and threatens to also block Google if the company does not remove the video[25]. The Egyptian regulator however prevented a blocking of the video[26] as it that would have had ramifications on other Google services. The European Court of Human Rights ruled that the blocking of the entire Google Sites platform due to one hosted website violated freedom of expression rights[27].

PRIVACY AND DATA PROTECTION

TRANSNATIONAL DATA FLOWS REQUIRE COOPERATION

Discussions of how to govern transnational data transfers proliferate. Interoperability talks took place between Europe and the Asian-Pacific region to improve the compatibility of APEC's Cross-border Privacy Rules and the EU's Binding Corporate Rules[28]. In light of the planned EU data protection reform, the US also stressed the need of interoperability of national privacy standards[29]. In China, more comprehensive personal data protection guidelines were published[30].

Cross-border cooperation to enforce territorial privacy rules is on the rise as the Netherlands and Canada jointly investigate the California based chat tool WhatsApp[31] and several EU data protection authorities launch coordinated enforcement actions against Google's March 2012 Terms of Service update[32]. Germany allowed Facebook to continue the "real names" policy in its jurisdiction, but fined Google over its Street View WiFi data capture[34], while the UK reopened investigations[35] in the latter matter.

QUESTIONS

- How do diverse national privacy norms impact cross-border data flows?
- Given the dispersed jurisdictions involved in online interactions, will international cooperation on privacy issues increase?

DEFAMATION AND REPUTATION

MULTIPLE TAKEDOWN PROCEDURES?

In Germany, a court prescribed a notice and takedown regime for defamatory Google autocomplete suggestions[36]. Google is allowed not to pre-filter user generated content in the Italian jurisdiction[37], but can be liable for slow takedowns of defamatory content posted by users on Blogger in the UK[38]. The Brazilian legislature asks Google to establish a direct request process to delete potentially defamatory speech[39].

The Advocate General of the European Court of Justice suggests not acknowledging a ”right to be forgotten“ for results on a search engine[40]. In Ireland, home to major cross-border platforms' international headquarters, a court ordered an injunction to permanently remove a virally spreading video and enjoins the platforms and the plaintiff to discuss practical methods, whereas platforms demand that such a deletion should result only from a full trial[41].

New laws to tackle online defamation proliferate: a new defamation act that would limit ISP liability is underway in the UK[42]; a Swedish authority wants to criminalize grave online defamation[43]; Canada explores how to update its Criminal Code for cyberbullying[44] and a Mexican state adopted a broad new anti-cyberbullying law[45].

QUESTIONS

- How to deal with viral, transnational spreads of defamatory information?
- Is online defamation different from offline defamation and does it need special laws and procedures?
- What kind of judgment should be required for a complete removal of content? And, is it feasible?

TECHNOLOGIES

EXECUTION ERRORS AND CYBERTRAVEL LIMITATIONS

Enforcing national jurisdiction on the Internet can produce unintended consequences: an Australian financial regulator blocked 1200 websites instead of the intended two[46] and Italian law enforcement authorities blocked parts of Tumblr by accident[47]. Russia's social network VKontakte is blacklisted by error in some areas of the country[48].

Global limitations to cybertravel increase as the payment intermediaries Mastercard and Visa ban VPN providers[49] and China blocks certain VPN protocols[50]. Moreover, ISPs block Pirate Bay proxies in the UK[51], while assets of the operator of another Pirate Bay proxy are seized in the Dutch jurisdiction[52]. Internet switch offs continue to happen around the world as Syrian authorities shut down the national Internet for 20 hours[53] and India suspends the Internet in the Kashmir Valley to prevent the spread of viral rumors[54].

QUESTIONS

- How to ensure that website blockings do not produce negative unintended consequences on the whole network?
- What is the impact of VPN and proxy limitations on the geography of cyberspace?
- What norms are needed for domain seizures?

SECURITY

SURVEILLANCE AND CALLS FOR DATA SOVEREIGNTY

The revelations of the large-scale US National Security Agency's (NSA) Internet surveillance schemes Prism (access to user data stored by US-based cross-border online platforms)[55] and Fairview (direct "upstream" access to traffic in fibre optic cables)[56] to monitor global Internet communications appear to have long-term structural impacts on the ecology of cyberspace, including big data, cloud-computing, encryption and even the transnational routing of Internet traffic[57]. European debates on developing sovereign clouds[58] and establishing stronger privacy safeguards[59] gain momentum in the light of growing mistrust; the German Chancellor demands stricter global privacy rules[60] and Brazil discusses the notion of data sovereignty[61], the nationalization of data centers[62], as well as the creation of a new international agency to govern the Internet[63]. The Russian Senate calls for the creation of a UN agency to monitor the collection and use of personal data[64] and investigates Google for sharing Russian user data with US authorities[65].

Several lawsuits in the US[66], Germany, Luxembourg, Ireland[67], France[68] or the UK[69] challenge the NSA surveillance on issues ranging from violations of the right of association to the infringement of privacy laws in multiple jurisdictions. As a response, US-based platforms strive to release transparency statistics on NSA data requests[70]. Meanwhile, further online surveillance programs with extraterritorial reach are exposed in the UK[71], France[72] and Germany[73].

National jurisdictions strive to increase their lawful access to online interactions of their citizens: after India is granted access to BlackBerry data[74], it decided to ask Skype to set up local servers for the same purpose and considers the segregation of IP addresses on a state basis to facilitate targeted blocking in particular regions[75]. Likewise, Saudi Arabia is demanding access to Skype and WhatsApp communications in its jurisdiction and threatens to block these services otherwise[76].

QUESTIONS

- Will extraterritorial surveillance lead to stronger calls for data sovereignty?
- How to deal with the exercise of sovereignty over cross-border platforms and operators?
- How to ensure fair process and traceable procedures for access to user data?
- Is there a need for global privacy norms?
- What is the impact of extraterritorial surveillance on cloud computing and big data developments?

2. HOW TO ENABLE DIGITAL COEXISTENCE?

People from diverse jurisdictions cohabit in shared online spaces and interact across borders. Given this structural shift, can legal and regulatory tools based on separated national sovereignties efficiently handle transnational interactions in cyberspace, as well as the growing risk of normative collisions?

A 21ST CENTURY CHALLENGE
HANDLING DIVERSITY IN CYBERSPACE

The number of Internet users is said to have passed beyond 2.5 billions and will continue to grow at a rapid pace. Taking advantage of proliferating hosting and social-mediation services, they are able to easily post billions of pictures, blogs and videos, and interact in shared cross-border online spaces. From the onset, universal accessibility of online content and facilitation of interpersonal communication were the main benefits of the Internet and they deserve to be preserved.

Whereas transnational personal interactions are the exception in the physical world, they become the normal practice on the Internet. However, as the number of users increases, so does the heterogeneity of social, cultural, religious and political sensitivities, as well as the diversity of national legal norms that have to co-exist in cyberspace.

QUESTIONS

- How to enable Digital Coexistence?
- What frameworks can handle online interactions that simultaneously involve multiple jurisdictions (location of users, servers, platforms, TLD operators...)?

So far, the distributed and borderless architecture of the Internet has been maintained despite the diversity of users and norms. However, as the number of potential tensions and normative collisions will increase with the growing importance of the Internet, states are prompted to reaffirm their jurisdictional authority. Hence, the patchwork of applicable laws and potentially incompatible national procedures to enforce them is likely to become even more complex.

Is it possible to both maintain the social and economic benefits the cross-border Internet brings to mankind and ensure the peaceful Digital Coexistence of billions of people in cyberspace? Can existing inter-state frameworks for legal cooperation scale up? Or are new approaches needed to avoid re-aligning the network and its online services to national borders?

INTEROPERABILITY
CONNECTING HETEROGENEOUS ACTORS, NORMS AND PROCEDURES

Enabling Digital Coexistence in cross-border spaces requires transnational cooperation. However, traditional modes of cross-border cooperation between vertical legal systems lack clear procedural norms: every nation state has its distinct legal framework. A multitude of different procedures, which involve diverse actors and norms, exist to enforce national laws. Likewise, cross-border platforms and operators define in their Terms of Service private horizontal normative orders and make determinations on the compliance with national laws. The current situation results in legal uncertainty for public authorities, Internet platforms or operators and users alike. As a consequence, the need to enable the interoperability between the different vertical, as well as horizontal normative orders becomes crucial to avoid fragmentation.

QUESTIONS

- How to handle transnational online interactions and data flows in a Westphalian system?
- Will the transnational Internet be realigned to national subnets in the absence of appropriate procedural norms and interfaces?

Historical precedents provide relevant examples with regard to this challenge: the TCP/IP Protocols, the foundation of the Internet, allowed interoperability between heterogeneous networks and the HTML/HTTP Protocols, the foundation of the World Wide Web, enabled interoperability between heterogeneous databases. Likewise, Digital Coexistence requires frameworks and procedural standards to enable interoperability between heterogeneous stakeholders and normative orders across national borders.

Currently, there are no standardized mechanisms for the interface between public actors, operators and users regarding requests for domain seizures, content takedowns or access to user data. Direct requests from public authorities to Internet platforms or operators often rely on ad-hoc connections between actors along "trust networks". The traditional formal mode of international request routing would be Mutual Legal Assistance Treaties (MLATs). Being cumbersome and inappropriately slow for the digital age, MLATs do however not exist among all countries and are often limited to criminal issues.

QUESTIONS

- What procedural norms can ensure interoperability of heterogeneous systems?
- How to avoid a patchwork of incompatible procedures?
- How to ensure that smaller states, platforms or operators are not overlooked?

Thus, even when there is no conflict on the substance (i.e. dual incrimination, coherence between national requests and Terms of Service provisions, etc.), current frameworks are struggling to scale up to the quantity of requests, the diversity of actors and the multiplicity of normative orders involved. Moreover, fair process and accountability mechanisms need to be improved for both transnational public requests and private compliance determinations.

TENSIONS

ADDRESSING NORMATIVE COLLISIONS

Behavior that is legal in one country can be illegal in others, and different national norms can be incompatible or conflicting, for instance in their definition of hate speech. As the diversity of applicable rules on the Internet increases together with its global penetration, normative collisions are likely to grow in number and reach. Recent prominent cases include: global public order challenges, as with fears of ethnic violence in Assam enhanced by social media[77]; political tensions prompted by the "Innocence of Muslims" YouTube video[78]; or clashes between Terms of Service and national laws as with Twitter's initial reluctance to comply with a French court order for user data[79]. Moreover, normative collisions are also triggered by extraterritorial extensions of sovereignty, as seen with seizures of the Spanish Rojadirecta[80] domain by the US customs authorities, the seizure of servers of a globally used Bittorent platform[81] in the Ukrainian jurisdiction, or the US surveillance scheme Prism[82].

QUESTIONS

- What is the impact of unresolved normative collisions on the ecology of cyberspace and global Internet Governance?
- Is there a need for state-platform and user-platform dispute resolution?

The use of technical tools like geo-IP filtering and cc-TLD migrations may allow cross-border platforms to respect legal requirements in national jurisdictions without removing infringing content for users from other jurisdictions. Potential long-term consequences, however, include a progressive geographical fragmentation of shared online spaces. While neither the establishment of a detailed hierarchy of norms nor a global harmonization of Internet laws appear achievable, there is no framework today that can appropriately address normative collisions and diffuse the growing tensions. How and through which mechanisms should such transnational disputes be solved?

UNINTENDED CONSEQUENCES

THE COST OF INACTION

In the absence of proper interoperability frameworks that ensure Digital Coexistence, nation states, cross-border platforms and technical operators are likely to adopt uncoordinated and potentially incompatible solutions to manage problems resulting from the transnational nature of the Internet. Should this trend continue, it would ultimately result in a creeping fragmentation of the Internet and a forced re-alignment along national cyberspaces. This goes against the fundamental conception of the Internet as a distributed infrastructure allowing seamless transnational user interactions and services. Not only could this evolution jeopardize the benefits that Internet has brought to mankind, but it would also hamper innovation and growth. Among the potential costs of inaction are the following unintended consequences:

QUESTIONS

- Will the heterogeneity of public and private norms lead to a creeping fragmentation of cyberspace?
- What are the potential unintended consequences for the geography of cyberspace?

- Blocking
  Without procedures to granularly address content that may be illegal in their jurisdictions, states may adopt overly broad measures and block entire platforms based on their domains or IP addresses, reducing content availability.
- Filtering
  Faced with the challenge of compliance with potentially 190+ laws, cross-border platforms may generalize geo-IP filtering and automatic cc-TLD migrations to create localized experiences for users and therefore fragment transnational spaces for interaction.
- TLD Nationalization
  Following a global wave of domain seizures (e.g. the bodog case[83] in the US), companies and individuals might loose trust in global TLD registries and registrars located in foreign jurisdictions and retract to national operators instead, to the detriment of smaller countries.
- Jurisdictional Overstretch
  Given the unbalanced distribution of the physical location of operators, servers and cables, the unconstrained assertion of national authority in territories with global operators has extraterritorial effects on citizens of other countries. At the same time, some states might be unable to execute legitimate requests, in the absence of means to enforce national laws in online spaces used by their citizens.
- Forced Routing
  Due to concerns about surveillance programs (on US[84], UK[85] or German[86] territories), the principle of decentralized traffic routing might be challenged by the establishment of pre-defined links to route around certain jurisdictions, potentially harming the resilience of the whole network.
- Data Sovereignty
  The location of data matters. States increasingly consider enforcing national jurisdiction over server farms of cross-border online platforms[87] or hosting companies[88] located on their territory, or by creating data export barriers[89] and demand that their citizens' data be stored on national servers[90]. This can potentially endanger the viability of global cloud computing with its distributed server architectures.
- National Ecosystems
  Facing the limits of current frameworks to handle requests to cross-border online platforms or operators that are located in third countries, a growing number of states advocate the creation of national services[91] and sovereign clouds[92] in their jurisdictions. Moreover, states might oblige cross-border online platforms to establish local representations in every jurisdiction they are accessible in[93], which would represent a major challenge for start-ups and stifle their innovation capacities.

3. PROCEDURAL FRAMEWORKS FOR INTEROPERABILITY AND FAIR PROCESS

To diffuse tension and enable Digital Coexistence in cross-border online spaces, there is a growing understanding that some "procedural interfaces" between states, Internet operators or platforms and users need to be developed. The I&J dialogue process in 2013 allowed to map the following preliminary components and questions regarding possible procedural frameworks.

SCOPE

WHAT ISSUES NEED TO BE ADDRESSED?

At the very moment the situation described above calls for the development of "shared principles, norms, rules, decision-making procedures, and programmes", as specified in the Tunis Agenda for the Information Society (Article 34), it becomes all the more difficult to develop them precisely due to the growing heterogeneity. Enabling the Digital Coexistence of the diversity of people and legal norms in cyberspace requires new modes of cooperation and the development of innovative frameworks. Consensus emerges around a focus on three issue areas, which generate a high degree of tension:

- Domain Seizures
  How and in what situations should domain names be seized? What are the technical precautions?
- Content Takedowns
  How to ensure appropriate granularity and fair process when removing content from cross-border online platforms or making content inaccessible in certain jurisdictions?
- Access to User Data
  How to guarantee proportionality and traceability for law enforcement authorities' access to personal data?

QUESTIONS

- Is there a need for one overarching framework or separate, issue-based regimes?
- What are the most pressing issues likely to cause major tensions in the 21st century?
- How would fair process multi-stakeholder frameworks interface with existing "hard law"?

Such frameworks should not be limited to criminal cases, especially regarding content takedowns, and also allow handling the high quantity of "small cases". Moreover, procedural interfaces should address two distinct types of situations:

- Normative Coherence
  A request is legitimate, has a valid legal basis and is not in conflict with the provisions of cross-border platforms' Terms of Service or the law of their country of incorporation. In this case, requests should be routed efficiently, while ensuring fair process.
- Normative Collisions
  One party might regard a request as not fully legitimate or lacking a valid legal base. There can also be a tension between national laws and Terms of Service. In this case, there is a need for clear de-escalation procedures and possibly the creation of neutral dispute resolution processes.

BUILDING BLOCKS

WHAT FAIR PROCESS COMPONENTS?

The following six building blocks, which ensure trust, accountability and interoperability, could be further explored in discussions on fair process frameworks for cross-border online spaces:

- Authentication

  The identity of the sender and receiver of requests, be it states, users or operators, should be verifiable through appropriate "credentialing" mechanisms. This includes validating the authority of senders to issue a given request. Can a distinct naming and addressing system be developed for this purpose?
- Transmission

  There is a need for standardized submission formats to ensure unified comprehension of requests and to enhance the speed of their routing. Today, requests are transmitted in multiple formats via various mediums, including online portals, email, postal mail, fax and even diplomatic pouch.
- Traceability

  To foster accountability, it is important to facilitate the production of transparency reports; likewise logging of requests can enable ex-post audits or oversight.
- Determination

  What are the criteria for compliance with requests? Should operators themselves have to make determinations, or is there a need for neutral third-party validations?
- Safeguards

  Fair process must be ensured through quality assurances against quantitative and qualitative abuse, as well as notifications, contradictory procedures and appeals, when appropriate. Should a neutral body ensure oversight?
- Execution

  How should domains be seized, content be taken down and user information be transmitted in practice, in order to avoid harm to the infrastructure, guarantee proportionality and ensure accountability?

QUESTIONS

- Are other crucial building blocks missing?
- What sub-categories should each building block entail?
- What are the over-arching principles under which fair process components would be implemented?

THE WAY FORWARD

HOW TO DEVELOP SUCH FRAMEWORK(S)?

Three elements are fundamental for the process of developing appropriate fair-process frameworks for cross-border online spaces to handle Digital Coexistence:

- Inclusion

  The traditional Westphalian model of purely inter-governmental cooperation is reaching its scalability limits due to the density of transnational interactions and multiplicity of jurisdictions involved in most online activities. Frameworks must be elaborated in a multi-stakeholder setting ensuring that a critical mass of states, international organizations, platforms, operators and civil society groups are involved in both the design and the implementation of procedural interfaces. This ensures balance, legitimacy and long-term viability of any fair-process framework(s).
- Geographic scope

  Traditional bilateral or multilateral MLATS work only linearly between states that negotiated these treaties. Therefore, they naturally lack flexibility and geographic reach. The objective for fair-process frameworks is to ultimately enable wide adoption and geographic scalability. It is therefore important to engage actors from various regions from the onset to facilitate ulterior participation in any potential regime. Legitimacy depends upon taking the diversity of perspectives into account.
- Instruments

  Fair process framework(s) could be developed in the form of guidelines or principles, but this would insufficiently guarantee basic needs for enforceability. Equally, traditional treaties and conventions might not be appropriate instruments, since intergovernmental negotiation processes can be very long and too static to cope with the high pace of innovation in the ecology of cyberspace. Therefore, it might be appropriate to explore new instruments of governance, such as Mutual Affirmations of Commitments involving the different categories of actors by defining their respective roles and responsibilities.

QUESTIONS

- How to guarantee the legitimacy of multi-stakeholder process frameworks?
- How to ensure the scalability of any potential interoperability regime?
- What are appropriate instruments to establish procedural interfaces between state, operators and users?

ANNEX/REFERENCES

COPYRIGHT

1 Guardian (13.2.2013). When does freedom of speech trump copyright? http://www.guardian.co.uk/media-network/media-network-blog/2013/feb/13/freedom-speech-trump-copyright

2 ArsTechnica (13.3.2013). European Court of Human Rights unanimously rejects Pirate Bay appeal. http://arstechnica.com/tech-policy/2013/03/european-court-of-human-rights-unanimously-rejects-pirate-bay-appeal/

3 TorrentFreak (26.2.2013). The Pirate Bay departs Sweden and sets sails for Norway and Spain. https://torrentfreak.com/the-pirate-bay-departs-sweden-and-sets-sail-for-norway-and-spain-130225/

4 TorrentFreak (25.4.2013). Pirate Bay finds safe haven in Iceland, switches to.IS domain. https:t//torrentfreak.com/pirate-bay-finds-safe-haven-in-iceland-switches-to-is-domain-130425/

5 Tecmondo (20.5.2013). Brasil: Google deve excluir conteúdo plagiado mesmo sem ordem judicial.

6 TechDirt (25.6.2013). SOPA didn't die, it just emigrated. https://www.techdirt.com/articles/20130625/09171223611/sopa-didnt-die-it-just-emigrated-to-russia.shtml

7 Future of Copyright (2.6.2013). Italian court: seizure of file sharing website disproportionate. http://www.futureofcopyright.com/home/blog-post/2013/06/03/italian-court-seizure-of-file-sharing-website-disproportionate.html

8 ZDNet (25.4.2013). CISPA 'dead' in Senate, privacy concerns cited. http://www.zdnet.com/cispa-dead-in-senate-privacy-concerns-cited-7000014536/

9 Read Write Web (12.3.2013). How your ISP will take six strikes at suspected pirates. http://readwrite.com/2013/03/12/isp-six-strikes-anti-piracy-system-infographic

10 ArsTechnica (3.6.2013). France removes Internet cut-off threat from its anti-piracy law. http://arstechnica.com/tech-policy/2013/06/france-removes-internet-cut-off-threat-from-its-anti-piracy-law/

11 TorrentFreak (13.6.2013). France disconnects first file-sharer from the Internet. https://torrentfreak.com/france-disconnects-first-file-sharer-from-the-internet-130613/

FREEDOM OF EXPRESSION

12 New York Times (12.7.2013). Twitter yields to pressure in hate case in France. http://www.nytimes.com/2013/07/13/technology/twitter-yields-to-pressure-in-hate-case-in-france.html

13 Times of India (14.6.2013). Twitter urged to reveal identities of 'racist' users. http://articles.timesofindia.indiatimes.com/2013-06-15/social-media/39992327_1_racist-tweets-rights-groups-appeal

14 Read Write Web (4.12.2012). Twitter gets ready to open its new offices in France. http://thenextweb.com/twitter/2012/12/04/twitter-is-ready-to-open-its-new-offices-in-france/

18 Reuters (26.6.2013). Turkey seeks to tighten grip on Twitter after protests. http://www.reuters.com/article/2013/06/26/turkey-protests-twitter-idUSL3N0F22TQ20130626

19 New York Times (28.5.2013). Facebook says it failed to bar posts with hate speech. http://www.nytimes.com/2013/05/29/business/media/facebook-says-it-failed-to-stop-misogynous-pages.html

20 Economist (23.4.2013). Why does liberal Iceland want to ban online pornography? http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-why-iceland-ban-pornography

21 LA Times (4.4.2013). Egypt moves to block access to pornography. http://articles.latimes.com/2013/apr/04/world/la-fg-wn-egypt-access-pornography-20130404

22 Hindu (24.3.2013). Steps taken to block 600 porn sites, court told. http://www.thehindu.com/todays-paper/tp-national/tp-kerala/steps-taken-to-block-600-porn-sites-court-told/article4543548.ece

23 Hyperderecho (25.7.2013). Proyecto de Ley propone establecer una censura previa en Internet. http://www.hiperderecho.org/2013/07/proyecto-de-ley-propone-establecer-una-censura-previa-en-internet/

24 Independent (22.7.2013). UK ISPs to filter porn by default by year's end. http://www.pcmag.com/article2/0,2817,2422063,00.asp

25 Times of India (18.7.2013). Pakistani officials: No tech to block blasphemous content on web. http://articles.timesofindia.indiatimes.com/2013-07-18/internet/40655899_1_pakistan-telecommunication-authority-blasphemous-content-youtube

26 Reuters (14.2.2013). Egyptian regulator appeals against court's YouTube ban. http://www.reuters.com/article/2013/02/14/net-us-egypt-youtube-idUSBRE91804Q20130214

27 UK Human Rights Blog (16.1.2013). Turkish block on Google site breached Article 10 rights, rules Strasbourg. http://ukhumanrightsblog.com/2013/01/16/turkish-block-on-google-site-breached-article-10-rights-rules-strasbourg/

PRIVACY AND DATA PROTECTION

28 CNIL (21.2.2013). International data transfers: towards an articulation of data flow systems between Europe and the Asia-Pacific area? http://www.cnil.fr/english/news-and-events/news/article/international-data-transfers-towards-an-articulation-of-data-flow-systems-between-europe-and-the-as/

29 EurActive (23.4.2013). US makes first public comment over draft EU data privacy law. http://www.euractiv.com/infosociety/us-airs-views-eu-privacy-rules-news-519279

30 DLA Piper (8.2.2013). China's evolving personal data privacy landscape. http://www.dlapiper.com/zh-CHS/china/publications/detail.aspx?pub=7857

31 OPC & CBC (28.1.2013). WhatsApp's violation of privacy law partly resolved after investigation by data protection authorities. http://www.cbpweb.nl/downloads_pb/pb_20130128-whatsapp-opc-cbp-newsrelease-en.pdf

32 Bloomberg (24.6.2013). France, Spain and UK open enforcement actions against Google. http://www.bna.com/france-spain-uk-n17179874716/

33 Techcrunch (15.2.2013). Facebook wins court challenge in Germant against its real names policy. http://techcrunch.com/2013/02/15/facebook-wins-court-challenge-in-germany-against-its-real-names-policy/

34 BBC (22.4.2013). Google fined over illegal wi-fi data capture in Germany. http://www.bbc.co.uk/news/technology-22252506

35 ZDNet (13.6.2013). Google Wi-Fi snooping probe back on despite deletion of vital data. http://www.zdnet.com/google-wi-fi-snooping-probe-back-on-despite-deletion-of-vital-data-3040155376/

DEFAMATION AND REPUTATION

36 SearchEngineLand (14.5.2013). German court says Google must block libelous words added via autocomplete function. http://searchengineland.com/germany-says-google-must-block-libelous-words-added-with-autocomplete-function-159436

37 Reuters (27.2.2013). Google not expected to check every upload says Italian court. http://www.reuters.com/article/2013/02/27/net-us-google-italy-privacy-idUSBRE91Q0TP20130227

38 Guardian (14.2.2013). Google must act quickly on libelous Blogger posts, says appeal court. http://www.guardian.co.uk/media/2013/feb/14/google-libel-blogger-posts

39 Knight Center for Journalism in the Americas (22.3.2013). Brazilian legislature proposes plan to streamline removal of defamatory content online. https://knightcenter.utexas.edu/blog/00-13264-brazilian-legislature-proposes-plan-streamline-removal-defamatory-content-online

40 Globe and Mail (25.6.2013). Google doesn't have to delete sensitive information from search index: EU court adviser. http://www.theglobeandmail.com/technology/google-not-required-to-delete-sensitive-information-from-search-index-eu-court-adviser/article12792975/

41 Independent (20.6.2013). Net giants want full trial over defamatory video order. http://www.independent.ie/irish-news/courts/net-giants-want-full-trial-over-defamatory-video-order-29358922.html

42 Huffington Post (25.6.2013). The new defamation Act: Game changer or red herring? http://www.huffingtonpost.co.uk/shana-ting-lipton/the-new-defamation-act-ga_b_3466158.html

43 IDG (14.1.2013). Swedish authority wants online defamation to be punishable by law. http://news.idg.no/cw/art.cfm?id=47C7775E-B87C-00DF-13D5CE1C-42DADBAE

44 Brampton Herald (24.7.2013). Cyberbullying report calls for Criminal Code changes. http://www.bramptonguardian.com/news-story/3905482-cyberbullying-report-calls-for-criminal-code-changes/

45 Global Voices (3.6.2013). Mexico: Local cyberbullying law could threaten free expression. http://advocacy.globalvoicesonline.org/2013/06/03/mexico-local-cyberbullying-law-could-threaten-free-expression/

TECHNOLOGIES

46 Delimiter (15.5.2013). Interpol filter scope creep: ASIC ordering unilateral website blocks. http://delimiter.com.au/2013/05/15/interpol-filter-scope-creep-asic-ordering-unilateral-website-blocks/

47 EDRi (27.2.2013). Italian police blocks Tumblr domain. http://www.edri.org/edrigram/number11.4/italy-blocks-tumblr-domain

48 BBC (24.5.2013). Error blacklists Russia's top social network VKontakte. http://www.bbc.co.uk/news/world-europe-22651973

49 Register (4.7.2013). Mastercard and Visa block payments to Swedish VPN firms. http://www.theregister.co.uk/2013/07/04/payment_block_swedish_vpns/

50 Guardian (14.12.2012). China tightens 'Great Firewall' internet control with new technology. http://www.guardian.co.uk/technology/2012/dec/14/china-tightens-great-firewall-internet-control

51 MusicWeek (12.6.2013). UK ISPs block host of new Pirate Bay proxy sites. http://www.musicweek.com/news/read/uk-isps-block-host-of-new-pirate-bay-proxy-sites/055009

52 TorrentFreak (3.4.2013). Pirate Bay proxy owner's bank account seized by anti-piracy group. https://torrentfreak.com/pirate-bay-proxy-owners-bank-account-seized-by-hollywood-group-130403/

53 ZDNet (7.5.2013). Report: Syria cut off from the Internet once again. http://www.zdnet.com/report-syria-cut-off-from-the-internet-once-again-7000015029/

54 Times of India (18.7.2013). Internet services suspended in Kashmir Valley. http://articles.timesofindia.indiatimes.com/2013-07-18/internet/40656015_1_internet-services-mohammad-afzal-guru-kashmir-valley

SECURITY

55 New York Times (6.6.2013). US confirms that it gathers online data overseas. http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html

56 Gizmodo (12.7.2013). Let's talk about Fairview, the NSA's plan to "own the Internet". http://gizmodo.com/lets-talk-about-fairview-the-nsas-plan-to-own-the-i-758300897

57 CircleID (18.6.2013). Provoking National Boundaries on the Internet? A chilling thought… http://www.circleid.com/posts/20130618_provoking_national_boundaries_on_the_internet_a_chilling_thought/

58 GigaOM (4.7.2013). European PRISM anger gains momentum with fresh cloud warnings and data threats. http://gigaom.com/2013/07/04/european-prism-anger-gains-momentum-with-fresh-cloud-warnings-and-data-threats/

59 ZDNet (15.7.2013). PRISM: EU renews efforts to get US to recognise citizens' right to privacy. http://www.zdnet.com/prism-eu-renews-efforts-to-get-us-to-recognise-citizens-right-to-privacy-7000018072/

60 NPR (14.7.2013). Merkel Urges Stronger Europe, Global Data Rules. http://www.npr.org/templates/story/story.php?storyId=202070025

61 Convergencia Digital (11.7.2013). Marco Civil não ataca "grampos", mas vai incluir soberania de dados. http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34263&sid=11#.UfKFM1NSZry

62 Tecmundo (13.7.2013). Brasil quer nacionalizar servidores e preocupa empresas de internet. http://www.tecmundo.com.br/internet/41948-brasil-quer-nacionalizar-servidores-e-preocupa-empresas-de-internet.htm#ixzz2anAXfR7X

63 Globo (8.7.2013). Ministro diz não ter dúvida de que EUA espionaram brasileiros. http://g1.globo.com/politica/noticia/2013/07/ministro-diz-nao-ter-duvida-de-que-eua-espionaram-brasileiros.html

64 New York Times (14.7.2013). NSA leaks revive push in Russia to Internet control. http://www.nytimes.com/2013/07/15/business/global/nsa-leaks-stir-plans-in-russia-to-control-net.html

65 Ria Novosti (24.7.2013). Google to talk to Russian senators over data leak probe. http://en.ria.ru/russia/20130724/182393940/Google-to-

Talk-to-Russian-Senators-Over-Data-Leak-Probe.html

66 EFF (16.7.2013). Unitarian Church, gun groups join EFF to sue NSA over illegal surveillance. https://www.eff.org/press/releases/unitarian-church-gun-groups-join-eff-sue-nsa-over-illegal-surveillance

67 ArsTechnica (26.6.2013). Students cite EU data protection laws, challenge firms over NSA data transfers. http://arstechnica.com/tech-policy/2013/06/students-cite-eu-data-protection-laws-challenge-firms-over-nsa-data-transfers/

68 Times of India (11.6.2013). US online snooping: Human rights groups file lawsuit in France. http://articles.timesofindia.indiatimes.com/2013-07-11/internet/40513699_1_rights-groups-lawsuit-human-rights-league

69 Guardian (8.6.2013). NSA and GCHQ spy programmes face legal challenge. http://www.guardian.co.uk/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge

70 Register (20.7.2013). Apple, Google, Facebook, Microsoft, world urge NSA transparency. http://www.theregister.co.uk/2013/07/20/tech_titans_urge_more_government_snopping_transparency/

71 Wired (24.6.2013). A simple guide to GCHQ's Internet surveillance programme Tempora. http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101

72 BBC (4.6.2013). France 'has vast data surveillance' - Le Monde report. http://www.bbc.co.uk/news/world-europe-23178284

73 Phoenix (3.7.2013). Der BND sammelt Daten am Internetknoten DE-CIX in Frankfurt. http://www.phoenix.de/content//713040

74 IT Pro (15.7.2013). BlackBerry gives Indian government "lawful" access to user data. http://www.itpro.co.uk/mobile/20193/blackberry-gives-indian-government-lawful-access-user-data#ixzz2aA7CGIiv

75 Times of India (20.5.2013). Government wants Skype to set up servers in India. http://articles.timesofindia.indiatimes.com/2013-05-20/infrastructure/39391625_1_internet-telephony-law-enforcement-servers

76 AlArabia (31.3.2013). Saudi Arabia threatns to block Skype, WhatsApp, Viber. http://english.alarabiya.net/en/2013/03/25/-Saudi-Arabia-threatens-to-block-Skype-WhatsApp-Viber.html

HOW TO ENABLE DIGITAL COEXISTENCE?

77 The Economic Times (23.12.2012). Government blocks Twitter handles of journalists, right-wing groups. http://articles.economictimes.indiatimes.com/2012-08-23/news/33342537_1_twitter-accounts-twitter-users-block-six-fake-accounts

78 New York Times (14.9.2012). Google has no plans to rethink video status. http://www.nytimes.com/2012/09/15/world/middleeast/google-wont-rethink-anti-islam-videos-status.html

79 ZDNet (15.7.2013). Twitter finally hands over details of accounts used to post racist tweets. http://www.zdnet.com/twitter-finally-hands-over-details-of-accounts-used-to-post-racist-tweets-7000018044/

80 ArsTechnica (29.8.2012). Government admits defeat, gives back seized Rojadirecta domains. http://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/

81 TorrentFreak (6.12.2012). Demenoid busted as a gift to the United States government. https://torrentfreak.com/demonoid-busted-as-a-gift-to-the-united-states-government-120806

82 ZDNet (21.6.2013). Amid NSA spying scandal, the gloves are off for EU's justice chief. http://www.zdnet.com/amid-nsa-spying-scandal-the-gloves-are-off-for-eus-justice-chief-7000017132/

83 Michael Geist (6.3.2012). All your Internets belong to the US, continued. http://www.michaelgeist.ca/content/view/6359/135/

84 Guardian (11.6.2013). Boundless Informant: The NSA's secret tool to track global surveillance data. http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining

85 Guardian (21.6.2013). GCHQ taps fibre-optic cables for secret access to world's communications. http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

86 Netzpolitik (2.7.2013). "BND has access to German Internet Exchange Point DE-CIX" https://netzpolitik.org/2013/bnd-hat-zugriff-auf-deutschen-internet-knoten-de-cix/

87 New York Times (7.12.2012). Dismayed at Google's privacy policy, European group is weighing censure. http://www.nytimes.com/2012/12/08/technology/eu-panel-to-pressure-google-on-privacy-rules.html

88 Computerworld (3.10.2012). Swedish police confiscated three servers during raid on former Pirate Bay host. https://www.computerworld.com/s/article/9231979/Swedish_police_confiscated_three_servers_during_raid_on_former_Pirate_Bay_host

89 Convergencia Digital (11.7.2013). "Marco Civil will include data sovereignty". http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34263&sid=11#.UelH3FNSZrz

90 Times of India (20.5.2013). Government wants Skype to set up servers in India. http://articles.timesofindia.indiatimes.com/2013-05-20/infrastructure/39391625_1_internet-telephony-law-enforcement-servers

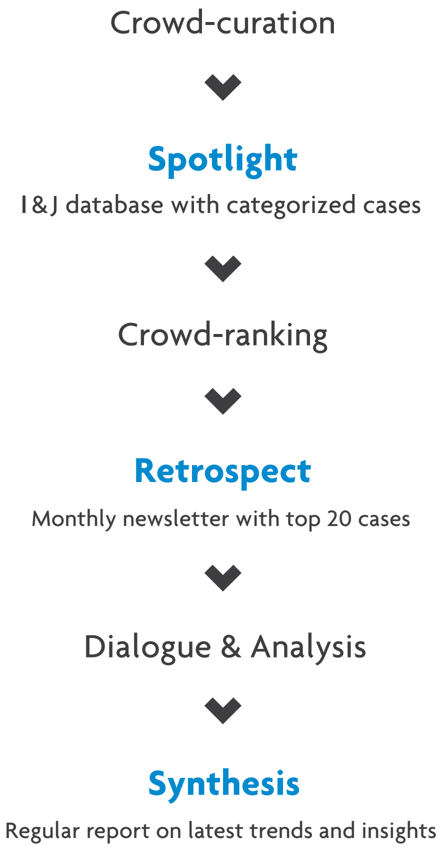
91 BBC (27.4.2013). Will Iran's national internet mean no world wide web? http://www.bbc.co.uk/news/world-middle-east-22281336

92 Reuters (17.6.2013). European cloud computing firms see silver lining in PRISM scandal. http://www.reuters.com/article/2013/06/17/us-cloud-europe-spying-analysis-idUSBRE95G0FK20130617

83 BBC (27.6.2013). Turkey seeks to tighten control over Twitter. http://www.bbc.co.uk/news/technology-23079607

THE INTERNET & JURISDICTION OBSERVATORY

Over 20 selected international experts support the Internet & Jurisdiction Project in keeping track of important trends around the globe. The monthly Retrospect newsletter and the bi-annual Synthesis inform participants of the multi-stakeholder dialogue process about the latest cases and dynamics via a progressive, crowd-curated filtering process.


Crowd-curation
Spotlight
I & J database with categorized cases
Crowd-ranking
Retrospect
Monthly newsletter with top 20 cases
Dialogue & Analysis
Synthesis
Regular report on latest trends and insights

For more information, visit
www.internetjurisdiction.net/observatory/
and subscribe to our newsletter.

ABOUT

The Internet & Jurisdiction Project facilitates a global multi-stakeholder dialogue process to explore the tension between the technically borderless Internet and the patchwork of national jurisdictions.

Participants from states, international organizations, companies, civil society and the technical community are engaged in the dialogue process. The Internet & Jurisdiction Project provides a neutral platform to help frame the debate in a constructive manner and enables the discussion on the future of the cross-border Internet and jurisdiction.

Launched in January 2012, the Internet & Jurisdiction Project is organized in partnership with the International Diplomatic Academy.

FACILITATION TEAM

Bertrand de LA CHAPELLE
Project Director
bdelachapelle@internetjurisdiction.net

Paul FEHLINGER
Project Manager
fehlinger@internetjurisdiction.net

www.internetjurisdiction.net
Twitter : @IJurisdiction

INTERNET
& JURISDICTION
A GLOBAL MULTI-STAKEHOLDER
DIALOGUE PROCESS

ACADEMIE
DIPLOMATIQUE INTERNATIONALE

ADVANCING EFFECTIVE PRINCIPLED DIPLOMACY IN GOVERNMENT, BUSINESS AND CIVIL SOCIETY

The Internet & Jurisdiction Project has been made possible thanks to the financial support of: AFNIC (Manager of .fr), auDA (Manager of .au), NIC.br (Manager of .br), Google, Internet Society (ISOC), PIR (Manager of .org), Swiss Confederation – Federal Office of Communications (OFCOM), Verizon, Walt Disney Company